Dipartimento di Giurisprudenza *Cattedra di Informatica Giuridica*

IL CONTROLLO A DISTANZA NEI RAPPORTI DI LAVORO

RELATORE
Prof. Gianfranco Caridi

CANDIDATO
Marina D'Ascoli
Matr. 111133

CORRELATORE
Prof. Gianluigi Ciacci

ANNO ACCADEMICO 2016/2017

Introduzione

Capitolo Primo
Il controllo a distanza del datore di lavoro sul lavoratore.

1. Il potere di controllo del datore di lavoro ed il bilanciamento con l'esigenza di tutela della dignità e riservatezza. Cornice normativa.

1.1. Il potere di controllo nel Jobs Act (la modifica dell'art. 4 Stat. Lav.). Finalità della nuova normativa, prime considerazioni.

1.2. Excursus della norma.

2. Eliminazione del divieto di controllo come principio generale e considerazioni su tale inversione di tendenza.

3. Installazione degli strumenti di controllo ed impiego degli stessi: una distinzione prima non presente. Differenza terminologica tra installazione/impiego.

4. Tutela del patrimonio aziendale e controlli difensivi.

4.1. Legittimità dei controlli occulti.

5. Accordo sindacale e autorizzazione amministrativa. Modifiche apportate dal d.lg. 185/2016.

6. Distinzione tra “strumenti di controllo” e “strumenti di lavoro”. L’esempio del GPS.

6.1. Gli strumenti di rilevazione degli accessi e delle presenze.

7. Il nuovo comma 3 dell’art. 4 Stat. Lav. L’intreccio tra lo Statuto dei lavoratori e la disciplina della *privacy*.

8. Le condizioni di utilizzabilità dei dati. L’adeguata informazione.

8.1. Le condizioni di utilizzabilità dei dati. Il rispetto del Codice della privacy.

9. Le Linee guida del Garante in materia di posta elettronica e Internet.

10. L'utilizzabilità dei dati raccolti a fini disciplinari. Il caso Barbulescu v. Romania.

11. La protezione dei dati personali nell'ambito lavorativo. Il Regolamento UE 2016/679.

12. Lo *smart working*.

13. Controllo a distanza e *social network*.

14. Considerazioni conclusive circa le modifiche dell'art. 4 Stat. Lav.

Capitolo Secondo
Il controllo potenzialmente attuabile mediante strumenti informatici da parte di chiunque.

1. La vulnerabilità della tecnologia informatica e telematica al controllo.

2. Il sistema informatico e telematico quale ambito in cui si adempie il controllo.

3. Il controllo informatico potenzialmente messo in atto da parte di chiunque. Ragioni del controllo e strumenti informatici.

3-a) La potenzialità di controllo insita nella tecnologia informatica.

3-b) Possibili ragioni dell'atto di controllare ed eventuali conseguenze.
3-c) Alcuni strumenti informatici di cui avvalersi agevolmente al fine del controllo altrui.

3.1. Breve indagine su altre recenti ragioni del controllo informatico. Il fenomeno Anonymous e l'attivismo digitale.

3.1-a) Il fenomeno Anonymous quale esempio di intento di monitoraggio.

Introduzione.

All'interno di questo elaborato viene presentata la questione inerente al controllo a distanza nell'ambito della relazione lavorativa.

Più precisamente, ci si propone, nella prima parte, di analizzare tale peculiare forma di potere esercitata in particolar modo dal datore di lavoro sul lavoratore, individuabile nella compagine del potere direttivo datoriale.

La peculiarità sta nel fatto che si realizzi, in questi casi, un controllo definito "a distanza", il cui concetto fa riferimento sia alla distanza fisica che temporale, venendosi così a determinare la ininfluenza di contingenze quali il mancato funzionamento delle apparecchiature, la consapevolezza della loro presenza da parte dei lavoratori oppure l'utilizzo discontinuo delle stesse ai fini di controllo, i quali, dunque, non fungono da scriminanti all'applicazione della disciplina inerente.

La distanza è anche ciò che fa sì che il controllo possa realizzarsi in maniera insidiosa, talvolta occulta, a maggior ragione se si avvale di strumenti informatici e telematici.

Lo Statuto dei lavoratori dà una regolamentazione a tale fenomeno all'art. 4, che, con la riforma apportata dall'art. 23 del d.lgs. 14 settembre 2015, n. 151, è stato rinnovato in alcuni aspetti sia sostanziali che procedurali, per ciò che concerne gli impianti audiovisivi e gli altri strumenti dai quali possa derivare anche la possibilità di un controllo a distanza dell'attività lavorativa, compresi gli strumenti di lavoro e gli strumenti di registrazione degli accessi e delle presenze.

É stata proprio la diffusione e pervasione della tecnologia digitale e dell'informatica nella vita lavorativa a richiedere la modifica dell'art. 4, il quale non poteva più prescindere da un aggiornamento reso necessario dall'esigenza di porre la norma al passo con i tempi.

Infatti, al giorno d'oggi, il controllo è un atto al quale dedicare maggiore attenzione d'analisi nell'ambito lavorativo, poiché si è arrivati, in virtù dell'evoluzione tecnologica, al punto in cui esso è realizzabile per il tramite di mezzi che costituiscono, al tempo stesso, strumenti impiegati dal lavoratore per rendere la sua prestazione, andando a determinare la possibilità per il datore di lavoro di addentrarsi nella vita privata del lavoratore in modo più insidioso rispetto ad un recente passato.

Tutto ciò pur sempre in considerazione del fatto che il controllo operato dal datore di lavoro trovi comunque la sua limitazione nell'esigenza del lavoratore di vedersi riconosciuta la tutela alla dignità ed alla riservatezza, innescando quella delicata ricerca di un necessario bilanciamento tra le contrapposte esigenze delle parti.

Si è, quindi, ritenuto doveroso stabilire che la vigilanza attuata sul lavoratore, ancorchè necessaria nell'organizzazione produttiva, andasse mantenuta in una dimensione umana, ossia non esasperata dall'uso di tecnologie suscettibili di rendere l'opera di monitoraggio continua ed anaelastica,

suscettibile, in questo modo, di eliminare ogni zona di riservatezza e di autonomia nello svolgimento del lavoro.

A tal proposito, un ruolo centrale è stato ed è svolto dalla giurisprudenza, la quale è riuscita ad indicare di volta in volta quali fossero i limiti da porre al potere di controllo e le modalità per un suo lecito esercizio, consentendo, in tal modo, alla norma dello Statuto di confrontarsi con le innovazioni tecnologiche e di rispondere alle nuove esigenze che, nel tempo, si sono andate affermando nel mondo del lavoro.

Inoltre, si individua, alla luce del dettato della nuova disposizione statutaria, l'intreccio tra due distinte normative, la disciplina lavoristica e la disciplina della *privacy*, funzionale, nell'intento del Legislatore, alla realizzazione di una moderna tutela dei diritti di dignità e riservatezza del lavoratore.

Alcune considerazioni finali, inerenti alla prima parte, riguardano il controllo a distanza eventualmente effettuato mediante i *social network* ed il fenomeno dello *smart working*, nella constatazione della necessità di dare attuazione alla normativa di cui all'art. 4 anche in riferimento a tali nuovi ambiti in cui si adempie l'attività lavorativa.

La seconda parte dell'elaborato presenta quale oggetto di indagine l'attività di controllo potenzialmente messa in atto, mediante strumenti informatici, da parte di chiunque e, su tale premessa, viene vagliata l'ipotesi del possibile controllo effettuabile da parte del lavoratore sul proprio datore di lavoro.

Di quest'ultimo caso, ne viene valutata l'inopportunità sulla base delle norme che regolano i doveri che il lavoratore è tenuto a rispettare, in vista della collaborazione all'interno dell'organizzazione e gestione del lavoro aziendale e dell'utilità reciproca, cui è indirizzata l'attività di una parte nei confronti dell'altra, al fine di un corretto svolgimento della prestazione e di un ottimale risultato produttivo.

Un altro ordine di considerazioni è dedicato alla rilevazione dell'impatto che le nuove tecnologie dell'informazione e della comunicazione possono avere sia in ambito politico che in ambito sindacale. Da qui la breve indagine svolta sull'attivismo digitale e la delineazione di un possibile impiego di tali tecnologie anche da parte del sindacato, a condizione di una reale presa di coscienza e comprensione delle nuove tendenze che stanno caratterizzando il mondo del lavoro.

L'analisi effettuata nella sua interezza sul fenomeno del controllo, messo in atto nell'ambito della relazione lavorativa, è volta, in ogni caso, a far emegere l'importanza e la necessità dell'opera di bilanciamento tra gli interessi contrapposti delle parti contrattuali, costantemente svolta, dal Legislatore, dalla giurisprudenza e dall'interprete, sia nel caso, normato dal riformato art. 4 Stat. Lav., della possibilità da parte del datore di lavoro di compiere un controllo a distanza dell'attività

dei lavoratori e sia nel caso inverso di un eventuale controllo da parte del lavoratore sull'attività del datore di lavoro e sulle informazioni ad essa relative.

Capitolo Primo

Il controllo a distanza del datore di lavoro sul lavoratore.

1. Il potere di controllo del datore di lavoro ed il bilanciamento con l'esigenza di tutela della dignità e riservatezza. Cornice normativa.

Tra i poteri del datore di lavoro rientra quello di controllare l'esatta esecuzione della prestazione lavorativa dovutagli, verificando se il dipendente usi la prescritta diligenza e osservi le disposizioni impartitegli, anche al fine dell'eventuale esercizio del potere disciplinare.

Tali poteri trovano un primo fondamento normativo negli artt. 2104, 2105, 2106 del Codice civile.

Nell'ambito del rapporto lavorativo, il potere di controllo è ritenuto connaturato alla posizione contrattuale del datore di lavoro, giacché, da solo il potere direttivo non potrebbe garantire la piena e sicura realizzazione dell'interesse a ricevere la prestazione.

Occorre tuttavia rilevare come l'implicazione del lavoratore (inteso come persona) nello svolgimento della prestazione possa determinare il concreto pericolo che il controllo possa essere esercitato in modo lesivo di diritti fondamentali quali la dignità e la riservatezza del lavoratore.[1]

Ed infatti, se da un lato la titolarità in capo al datore di lavoro di un potere di controllo è caratteristica ontologica "immanente" del rapporto di lavoro[2], dall'altro, non è possibile trascendere dal fatto che la prestazione non può in alcun caso considerarsi un bene che esista al di fuori della persona del lavoratore, potendo essa essere attinta solo da lui stesso, in quanto inseparabilmente legata all'uomo che lavora[3].

Da qui la considerazione secondo la quale gli aspetti della vita privata del lavoratore possano, in maniera più o meno incisiva, influenzare l'adempimento della prestazione lavorativa tanto da rendere imprescindibile la necessità di un controllo ai fini di garantire il rapporto sinallagmantico.

Stante la "necessità" del controllo come sopra individuata è necessario pertanto individuare ed esplorare i confini di questo potere riconosciuto al datore di lavoro.

A tracciare i primi limiti di questo potere è stata innanzitutto la Costituzione, che in alcuni suoi articoli va a tutelare in generale la persona e la sua libertà di autodeterminazione (artt. 2, 13, 14, 15, 21 Cost.).

---

1 A. VALLEBONA, *Breviario di diritto del lavoro*, sesta edizione, Giappichelli, Torino, 2010, 270 ss.

2 G. GHEZZI, U. ROMAGNOLI, *Il rapporto di lavoro*, terza edizione, Zanichelli, Bologna, 1995, 217.

3 H. SINZHEIMER, *La democratizzazione del rapporto di lavoro*, *Giornale di diritto del lavoro e delle relazioni industriali*, 1979, 217 ss.

Ulteriori e più precisi limiti al potere di controllo del datore di lavoro sono enunciati dallo Statuto dei Lavoratori, il quale detta regole che hanno costituito la più significativa innovazione della legislazione italiana in materia di tutela delle informazioni personali con ampio anticipo rispetto all'emanazione della l. 31 dicembre 1996, n. 675[4].

Le premesse fin qui formulate valgono altresì per il potere di controllo specificamente disciplinato dall'art. 4 dello Statuto dei lavoratori., relativo al potere datoriale di controllo a distanza sull'operato del lavoratore, oggetto della presente trattazione.

Inoltre appare opportuno evidenziare sin da ora come tale tipo di controllo, ormai attuato dal datore di lavoro attraverso le nuove tecnologie, tocchi senza alcun dubbio, ed oggi in maniera ancor più pressante, aspetti che attengono alla vita privata del lavoratore: lo strumento tecnologico risulta infatti, contemporaneamente, mezzo per svolgere la prestazione lavorativa e mezzo di controllo nelle mani del datore di lavoro.

Sotto questo ultimo profilo, inoltre, si rileva come la possibilità di raccogliere dati sui suoi dipendenti permetta al datore di lavoro di ricostruire un profilo particolarmente preciso del lavoratore, potendo conoscerne le abitudini, opinioni e orientamenti.

Si è, per tale ragione, sottolineato che la vigilanza sul lavoratore, ancorchè necessaria nell'organizzazione produttiva, va mantenuta in una dimensione umana, 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[5].

Il fatto stesso che la disciplina in esame sia stata inserita nel Titolo I dello Statuto dei lavoratori, dedicato alla "Libertà e dignità del lavoratore", denota come il bene principalmente protetto dall'articolo debba essere identificato nella dignità del lavoratore, da intendersi come diritto del lavoratore a svolgere la propria prestazione in un ambiente sereno, libero da condizionamenti che potrebbero derivare da qualunque forma di controllo pressante e continuativo[6].

---

4 S. RODOTÀ , *Tecnologie e diritto*, Il Mulino, Bologna, 1995, 101.

5 Cass., sez. lav, sentenza 17 luglio 2007, n. 15982.

6 Osserva P. LAMBERTUCCI, in *Potere di controllo del datore di lavoro e tutela dellla 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", n. 235/2015, 5, che il lavoratore nel momento in cui stipula il contratto di lavoro non perde la connotazione di cittadino, con tutto il fascio di diritti costituzionalmente garantiti. Pertanto il confronto tra il potere di controllo del datore di lavoro nell'organizzazione dei diversi fattori della produzione e la tutela del lavoratore trova il suo momento di emersione normativa dapprima nella stessa Carta Costituzionale (art. 41 co. 2) e poi nel Titolo I dello Statuto dei lavoratori. Cfr. V. MAIO, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, *Argomenti di Diritto del Lavoro*, 6/2015, 1186 ss; M. T. CARINCI, *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D. Lgs. 151/2015): spunti per un dibattito*, *Labour&Law Issues*, vol. 2, n. 1, 2016.

In conclusione non si può fare a meno di considerare due aspetti inerenti alla disciplina del controllo a distanza e alla sua modifica: il primo è rappresentato dal necessario bilanciamento di due ordini di interessi, quello del datore di lavoro a ricevere la prestazione a lui dovuta e alla verifica legittima affinchè questa venga svolta nel modo dovuto (secondo quanto stabilisce il codice civile); il secondo è l'interesse del lavoratore a vedere riconosciuta una tutela alla sua dignità e riservatezza, poiché il lavoratore prima di essere tale è soprattutto una persona con i suoi diritti, tra i quali quello fondamentale alla *privacy*.

A questo proposito la norma statutaria, sia nella sua precedente veste, ma anche e soprattutto nella nuova, deve tenere in considerazione la ricerca di questo importante equilibrio, non dimenticando che, nell'ambito del rapporto di lavoro, il contemperamento tra questi diritti deve essere modulato sulla base dell'oggetto del contratto e cioè del concreto contenuto della prestazione di lavoro dovuta e del coinvolgimento dei valori della persona che l'adempimento della mansione postula.

Un ulteriore aspetto sul quale si vuole porre l'accento è quello contingente al momento normativo attuale e alle ragioni che hanno condotto alla modifica della norma, la quale ha dovuto prendere atto, nella sua nuova formulazione, del cambiamento tecnologico che la società dell'informazione ha portato con sé.

Si vede così che, per quanto parte della dottrina avesse già individuato una carenza dell'articolo 4 nello stare al passo coi tempi[7], il problema della riservatezza *stricto sensu*, alla quale la persona-lavoratore ha diritto, sia emersa in maniera evidente solo a partire dal momento in cui le tecnologie impiegate dal datore di lavoro si sono rivelate idonee ad acquisire anche informazioni rientranti nella vasta area dei dati personali e sensibili del lavoratore.

Basti pensare alle potenzialità insite nell'impiego del *personal computer*, della rete internet e della posta elettronica nella quotidianità lavorativa, per accorgersi di come l'interrogazione dei dati registrati da questi strumenti consenta anche l'acquisizione di informazioni private come quelle derivanti ad esempio dalla lettura di eventuali *e-mail* personali del lavoratore o dalla consultazione delle pagine Internet da lui visitate.

1.1 Il potere di controllo nel Jobs Act (la modifica dell'art. 4 Stat. Lav.). Finalità della nuova normativa, prime considerazioni.

Le regole dettate dall'art. 4 S. L. hanno subito delle modifiche, dopo oltre quarant'anni di vita, da parte dell'art. 23 del d.lgs. 14 settembre 2015, n. 151, intitolato " Semplificazioni in materia di

7 F. CARINCI, *Rivoluzione tecnologica e diritto del lavoro, Giornale di dir. del lav. e delle rel. indu.*, 1985, 224 ss. La norma statutaria non era in grado di reggere alle innovazioni tecnologiche, e quindi non poteva contrastare le potenzialità di controllo offerte al datore di lavoro dalla rivoluzione tecnologica.

lavoro e di pari opportunità", a sua volta promulgato in attuazione alla delega conferita al Governo dall'art. 1 co. 7 lett. f) della l. 10 dicembre 2014, n.183.

La finalità della modifica è quella di attuare 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 con la tutela della dignità e riservatezza del lavoratore.

In altri termini, tale disposizione non poteva più prescindere da un aggiornamento, reso necessario dall'esigenza di porre la norma al passo coi tempi, adeguandone il contenuto all'evoluzione tecnologica subita dalla società nel corso degli ultimi decenni.

Ed è proprio questa pervasione e diffusione della tecnologia e dell'informatica , resasi indispensabile e quindi esponenziale, nella vita lavorativa a porre, urgente, la necessità di realizzare un ragionevole contemperamento tra l'interesse del datore di lavoro a controllare l'utilizzo da parte del lavoratore dei nuovi strumenti di lavoro e l'interesse del lavoratore a vedere protetta la propria dignità e riservatezza.[8]

Il cambiamento tecnologico, che ha necessariamente influenzato la modifica della normativa statutaria, ha enormemente ampliato e diffuso le capacità di controllo dell'attività dei lavoratori, specie attraverso modalità connettive di interazione a distanza a basso costo e capaci di operare di fatto senza soluzione di continuità. Si pensi a *smartphone* e/o *tablet* che, in tempo reale, comunicano il numero e la tipologia di interventi operati, ad esempio, da un tecnico piuttosto che da un commerciale, presso i clienti del datore di lavoro.

E' necessario prendere atto che la rilevanza delle innovazioni, apportate alla disciplina in materia di autorizzazione all'installazione e all'utilizzo degli impianti audiovisivi e degli altri strumenti di controllo a distanza, ad una prima analisi sembra aver accresciuto enormemente i poteri del datore di lavoro e aver inciso ancora di più sulla persona del lavoratore in termini limitativi della libertà e riservatezza, e dunque anche della sua dignità[9].

In questa direzione, inoltre, si è rilevato come la soluzione offerta dal nuovo art. 4 proponga "un punto di equilibrio a favore degli interessi dell'impresa, così avallandosi una portata espansiva dei

8 Dignità e riservatezza che si esprimono nel principio di tutela della vita privata del lavoratore nei confronti dell'imprenditore già insito nella disposizione che vieta all'iniziativa economica privata di svolgersi "in modo da recare danno alla sicurezza, alla libertà, alla dignità umana" (art. 41 Cost.) e nella disposizione che impone al datore di lavoro di adottare ogni misura necessaria a tutelare "la personalità morale del prestatore di lavoro" (art. 2087 c.c.).

9 G. VIDIRI, *Controlli datoriali sui dipendenti e tutela della privacy nel nuovo art. 4 Stat. Lav.*, *Il Corriere giuridico*, 11/2016, 1389 ss.

controlli difensivi anche perchè le informazioni assunte possono essere utilizzate a fini disciplinari"[10].

Un'altra considerazione sulla nuovo impianto normativo fa emergere come l'aspetto collettivo espresso dall'accordo sindacale (o autorizzazione amministrativa), richiesto dalla disciplina ai fini della concessione del potere di controllo datoriale, sia in qualche modo retrocesso lasciando spazio ad una gestione da parte dell'imprenditore più unilaterale degli strumenti attraverso cui si attua il controllo, e determinando una tutela, quindi, più sul piano individuale che collettivo anche grazie all'esplicito riferimento al diritto della *privacy*[11].

Infine, sotto il diverso versante della certezza del diritto, si è evidenziato anche come l'uso sempre più massiccio di strumenti tecnici di natura marcatamente polifunzionale (quali gli *smartphone* che consentono la geolocalizzazione del lavoratore che sia in possesso dell'apparecchio) renda ancora più labile la separazione tra la sfera personale e quella lavorativa, facendo diventare instabile qualunque approdo legislativo, che rischia così di ritrovarsi ad essere obsoleto prima ancora di diventare operativo[12].

1.2 Excursus della norma.

In questa sede si vuole, oltre che far emergere le novità scaturenti dalla normativa *post* riforma, provare ad individuare le ragioni e le conseguenze di questo cambio di prospettiva, attuato sì dal Legislatore, ma ovviamente innescato dall'evoluzione della società e dalle nuove e non ancora compiutamente delineate esigenze di "*privacy* digitale" dell'individuo.

Si fa subito presente che al primo comma dell'art. 4 il Legislatore ha eliminato l'esplicito divieto per finalità di controllo a distanza dell'attività dei lavoratori. Sparisce dunque il concetto di divieto

10 In questi termini F. SANTONI, *Controlli difensivi e tutela della privacy dei lavoratori*, *Giurisprudenza italiana*, 2016, 146.

11 "L'impressione che se ne ricava è un arretramento della centralità della tradizionale procedimentalizzazione sindacale (o amministrativa) dei poteri datoriali, funzionale al controllo di legittimità dell'installazione dell'impianto e radicata all'interno delle tradizionali categorie del diritto del lavoro, in favore di un modello che bilancia una gestione più unilaterale degli strumenti di controllo a distanza da parte dell'imprenditore (art. 4 co. 2) con inediti livelli di penetrazione del diritto della *privacy* nell'ambito del rapporto di lavoro (art. 4 co. 3). Ne deriva che il contemperamento dei diritti coinvolti tende oggi a realizzarsi su un piano più individuale che collettivo, per restare prevalentemente affidato alla disciplina del trattamento dei dati personali e quindi anche del potere regolamentare del Garante per la privacy." M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona", 300/2016, 5.

12 Così A. RONDO, *I controlli sulla posta elettronica del dipendente e l'art. 4 Stat. Lav. Prima e dopo il Jobs Act*, Massimario di Giurisprudenza del Lavoro, 2016, 41 ss. che cita F. GALGANO, *Lex mercatoria*, Il Mulino, Bologna, 1993, 234, ove afferma "l'inettitudine della legge alla innovazione giuridica".

assoluto di controllo, con tutta la sua portata densa di significato dal punto di vista della tutela del lavoratore, in particolar modo del riferimento alla sua persona e ai suoi diritti, e viene sostituito dal concetto di "permesso condizionato"[13]. In tale concetto sembra racchiuso tutto il nuovo impatto della norma, la quale disciplina espressamente le deroghe ad un divieto ormai divenuto implicito[14].

A differenza della precedente, la nuova disposizione non riproduce in esordio un esplicito divieto di installazione (e quindi di impiego) di impianti audiovisivi o di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori, essendo la prima parte del nuovo art. 4 dedicata alle regole d'installazione degli strumenti di controllo "preterintenzionale".

Nonostante l'impressione di netta discontinuità che può essere indotta dalla citata differenza di formulazione, si può però subito evidenziare che il divieto che la precedente formulazione enunciava espressamente può dirsi tuttora vigente, in quanto implicito nella regolazione contenuta nella norma riformata.

Il fatto che la nuova disposizione disciplini come un'eccezione l'installazione di strumenti dai quali derivi la possibilità di un controllo "preterintenzionale" dell'attività lavorativa, consente infatti di concludere agevolmente che deve ritenersi implicitamente vietata qualunque forma di controllo diretto dell'attività lavorativa tramite strumenti di controllo a distanza[15].

Tuttavia la nuova lettera normativa è stata anche letta nel senso di aver fatto retrocedere l'importanza posta sul divieto assoluto di controllo dalla sua posizione d'esordio, al punto da far "infuriare" i sindacati (Cgil) alla sua prima lettura[16].

Al nuovo comma primo inoltre si trova un'altra modifica rilevante relativa ad una delle esigenze che giustificano la possibilità di controllo a distanza dell'attività dei lavoratori, previo comunque l'accordo sindacale o l'autorizzazione amministrativa.

Si tratta dell'esplicita previsione, in aggiunta alle esigenze già presenti nel vecchio testo, della tutela del patrimonio aziendale.

---

13 M. T. GOFFREDO, V. MOSCA, *Jobs Act e nuovi controlli a distanza*, *Diritto & Pratica del Lavoro*, 31/2016, 1894ss.

14 Divieto, che giova ricordare, rimane granitico (i casi che ne consentono una deroga, previsti dal nuovo primo comma, sono preceduti dall'avverbio "esclusivamente", il quale fuga ogni dubbio circa una sua mancata previsione).

15 In tal senso si è espresso anche il Comitato dei Ministri degli Stati Membri del Consiglio d'Europa nella Raccomandazione CM/REc(2015)5 del 1° aprile 2015 sul trattamento dei dati personali nel contesto occupazionale. La Raccomandazione non ha un'efficacia vincolante per gli stati membri, ma una funzione di indirizzo nella prospettiva dell'adozione di una politica europea comune.

16 Così il segretario confederale della Cgil Sorrentino affermava, in data 18 giugno 2015, "Sui controlli a distanza siamo al colpo di mano. Il modo in cui è formulato l'articolo e la relazione illustrativa pongono un punto di arretramento pesante rispetto al precedente art. 4 legge 300".

Previsione che nelle intenzioni del Legislatore sembra voler portare chiarezza circa i contrasti dottrinali e giurisprudenziali insorti nel corso degli anni sui c.d. controlli difensivi sfociati in due orientamenti contrapposti.

Il primo sosteneva la non necessità di ottemperare alle procedure previste dal vecchio comma secondo nel caso appunto venissero messi in atto controlli relativi ai comportamenti del lavoratore lesivi del patrimonio e dell'immagine aziendale, laddove i divieti di cui all'art. 4 riguardassero il controllo sui modi di adempimento dell'obbligazione lavorativa. Sotto questo profilo non sarebbero vietati i c.d. controlli difensivi intesi a rilevare mancanze specifiche e comportamenti estranei alla normale attività lavorativa nonché illeciti; controlli eseguibili anche mediante agenzie investigative private (così Cass., sez. lav., sentenza 12 ottobre 2015, n. 20440).

L'opposto orientamento riteneva al contrario che anche i c.d. controlli difensivi dovessero rispettare la procedura di garanzia prevista dall'art. 4 (così Cass., sez. lav., sentenza 1° ottobre 2012, n. 16622).

In questo excursus della norma si pone poi in luce il cambiamento apportato dal nuovo comma secondo, la cui previsione ha suscitato un ampio dibattito sociale e politico, prima ancora che giuridico.

Più specificamente si fa riferimento al fatto che ora sia possibile, relativamente all'impiego di strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze, prescindere dall'accordo o autorizzazione previsti dal primo comma.

Infine la rivoluzione normativa si completa al comma terzo, ove la novità è duplice.

Da un lato, si stabilisce che le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro, quindi anche al fine di misurare il rendimento del lavoratore e/o di procedere all'irrogazione di sanzioni disciplinari, ponendo forti dubbi sul rispetto effettivo dei principi innanzitutto costituzionali di tutela della libertà e dignità del lavoratore.

Dall'altro lato, dopo aver apparentemente allargato le maglie del potere di controllo del datore di lavoro, pone un importante limite precisando che le informazioni così raccolte sono utilizzabili a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e tutto ciò nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

In questo modo il Legilatore pone tutta la normativa sotto l'ampio e rassicurante quanto discrezionale tetto della disciplina della *privacy*, comprendendo anche le pronunce del Garante, quasi volendo togliersi la responsabilità di un'azione legislativa che potrebbe configurarsi come distorsiva nei confronti delle prerogative dei lavoratori all'interno della disciplina del rapporto di lavoro, il quale ormai sembra voler rispondere a dinamiche ed esigenze (politiche, economiche) che

trascurano per forza di cose la tutela del singolo individuo, lasciata appunto ad una disciplina più generale che non può esularsi da tale compito[17].

Infine si vuole opportunamente precisare una questione di natura sistematica, inerente all'individuazione di tre fasi cronologicamente e funzionalmente distinte, che si palesano nel testo della nuova normativa. La prima riguarda l'acquisizione dei dati relativi all'attività lavorativa, come conseguenza automatica della tecnologia impiegata dal dipendente per svolgere la propria prestazione, la seconda concerne la conservazione dei dati, quindi la loro memorizzazione e la terza, eventuale, attiene all'utilizzazione dei dati raccolti per la gestione del lavoro (a tutti i fini connessi al rapporto di lavoro). Questa distinzione va a caratterizzare la tipologia dei controlli a distanza e delle prescrizioni ad essi inerenti corrispondenti ad ogni fase e viene operata al fine di permettere una migliore comprensione ed interpretazione delle novità da apportate alla normativa[18].

Si va, quindi, ora a trattare nel particolare ognuna di queste novità.

2. Eliminazione del divieto di controllo come principio generale e considerazioni su tale inversione di tendenza.

Non è possibile evitare di considerare che l'art. 4 ante riforma presentasse un esplicito e perentorio divieto di utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività del lavoratore.

In questo modo, l'originaro primo comma metteva fin da subito in evidenza quale fosse la finalità della norma, ossia quella di precludere assolutamente al datore di lavoro la possibilità di controllare con strumenti tecnologici lo svolgimento dell'attività lavorativa del dipendente, salvaguardando il suo spazio di riservatezza.

Questo divieto assoluto è stato rimosso dalla lettera della norma e sostituito da una formulazione contenente una disciplina positiva e compiuta dei casi e delle modalità in cui l'utilizzo degli strumenti di controllo è invece consentito, lasciando il divieto generale implicitamente inteso.

17 Si richiama l'evocativa immagine del bastone e della carota sapientemente utilizzati dal Legislatore secondo L. A. COSATTINI, *Le modifiche all'art. 4 Stat. Lav. Sui controlli a distanza, tanto rumore; per nulla?, Il Lav. nella giur*., 11/2015, 990.

18 A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in AA. VV. *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, Torino, 2017, 8.

Il cambiamento di prospettiva è evidente, sia da un punto di vista sociologico che metagiuridico, poiché un divieto implicito ha comunque, su tali piani, un peso diverso rispetto alla previsione di un divieto generale "sovrastante"[19].

Le ragioni di questo passo legislativo all'indietro possono essere ricondotte a vari piani che coinvolgono il nostro momento presente.

Viene a mente, innanzitutto, una ragione politica, laddove si voglia tenere in considerazione la situazione economica in cui si trova il nostro Paese.

L'Italia si pone come un paese ancora reduce di una pesante crisi economica che ha caratterizzato gli ultimi dieci anni e ne paga lo scotto nella ricerca di un continuo rilancio della sua economia.

Sono ormai lontani gli anni in cui l'Italia era la sesta potenza industriale al mondo ed il contesto politico ha appena cominciato ad accorgersene tanto da avere intrapreso la strada di un possibile rilancio economico basato sul principio di cercare di rendere l'Italia maggiormente appetibile agli investori stranieri, sino ad oggi allontanati dall'eccessiva burocrazia e dall'elevata tassazione.

Senza avere la pretesa di addentrarsi in speculazioni non attinenti all'argomento trattato, si vuole solo far emergere che uno degli aspetti che possono permettere un aumento della competitività del settore industriale è (anche) quello relativo all'impiego di strumenti di controllo al fine di monitorare il flusso della produttività dell'impianto aziendale, che è prodotto immediato dell'attività lavorativa che ogni dipendente esercita nell'ambito delle proprie mansioni.

In quest'ottica si inserisce il controllo del datore di lavoro, attuato al fine di garantire l'esatto compimento della mansione del lavoratore, che si pone quindi quale garanzia di produttività dell'impresa, non solo nell'interesse del singolo imprenditore, ma anche sul piano della produttività nazionale.

Da ciò è possibile dedurre come il concetto di controllo, negli ultimi anni, sia stato sempre più considerato e giustificato in virtù di obiettivi percepiti più alti all'interno della nuova scala gerarchica dei valori, che non vede più all'apice i bisogni dell'individuo, bensì un obiettivo di produttività e di competitività del Paese sul piano economico.

Un altro punto fondamentale, in questa ricerca delle ragioni metagiuridiche che possono aver condotto all'eliminazione del divieto esplicito di controllo da parte del Legislatore e quindi ad un cambiamento di prospettiva, è la presa di coscienza che il tema del potere di controllo da parte del

19 Sostiene L. A. COSATTINI: "Affermare che una certa attività è vietata e disciplinare poi i casi in cui a tale divieto è consentito derogare non è lo stesso che limitarsi a disciplinare (regolandoli) i casi in cui tale attività è consentita, se non altro per il fatto che nella prima fattispecie l'accento è posto sul divieto, mentre nella seconda l'attenzione è concentrata sui casi in cui l'attività è legittimamente esercitata. Non è una differenza di poco conto". In *Le modifiche dell'art. 4 Stat. Lav. sui controlli a distanza, tanto rumore; per nulla?,* i*l Lav. nella giur*., 11/2015, 985 ss.

datore di lavoro nell'impresa debba essere inevitabilmente riletto alla luce delle nuove potenzialità che la tecnologia offre.

Tale evoluzione ha determinato l'insorgere pratico di due interessi che per loro natura rappresentano le facce di una stessa moneta, ovvero, da un lato, l'espansione delle modalità di controllo del datore di lavoro (circostanza di per sé lesiva degli interessi del lavoratore) e, dall'altro, la necessità di tale controllo finalizzata alla verifica sulla produttività.

Infatti l'implementazione su larga scala delle moderne tecnologie informatiche ha determinato un'evoluzione dei modelli produttivi e organizzativi dell'impresa, generando scenari complessi in relazione ai quali l'esigenza del datore di lavoro di esercitare il potere di controllo ha assunto contorni nuovi.

Si può fare l'esempio dell'installazione della rete Internet, la quale comporta delle responsabilità per il datore di lavoro in quanto gestore della rete, che possono assumere anche una rilevanza penale.

Il controllo sugli accessi alla rete Internet e sui siti visitati può dunque essere richiesto dalla necessità di soddisfare tali nuove esigenze datoriali, anche se da tale controllo possono essere acquisite informazioni che riguardano dati sensibili del lavoratore[20].

Dunque, l'utilizzo da parte dei lavoratori del computer renderebbe "auspicabile" per il datore di lavoro la possibilità di controllare l'attività del dipendente con la finalità di evitare la commissione di reati informatici (ad esempio accesso a siti pedopornografici).

Rileva in tal senso il d.lgs. 8 giugno 2001, n. 231, novellato dalla l. 48/2008.

Tale decreto attribuisce una responsabilità degli enti collettivi in relazione alla commissione di determinati reati informatici, a fronte della quale emerge l'obbligo del datore di lavoro di predisporre adeguate tutele contro i rischi derivanti dalla navigazione in Internet e dall'uso della posta elettronica da parte dei dipendenti. Da ciò l'opportunità per l'ente collettivo di definire un adeguato modello organizzativo, recante "misure idonee a convincere il giudice penale a non ritenere ravvisabile una sua colpa di organizzazione, a partire dalla costituzione di un organismo di viglilanza dotato degli strumenti e dei poteri indispensabili per effettuare un continuo monitoraggio dello svolgimento delle attività informatiche dell'ente"[21].

20 I. ALVINO, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy, Labour&Law Issues*, vol. 2, n. 1, 2016, 10.

21 C. ZOLI, *Il controllo a distanza del datore di lavoro: l'art. 4, l. 300/1970 tra attualità ed esigenze di riforma*, *Riv. it. Dir. Lav*., 2009, I, 496; A. LEVI, *Il controllo informatico sull'attività del lavoratore*, Giappichelli, Torino, 2013, 7.

A ciò va aggiunto che un abuso delle strumentazioni informatiche da parte del lavoratore, che si sostanzi in una condotta lesiva della sfera morale nei confronti di un altro lavoratore, potrebbe esporre il datore di lavoro ad una responsabilità risarcitoria ai sensi dell'art. 2087 c.c.[22]

Il potere di controllo è quindi fatto oggetto di un'innegabile evoluzione tecnologica, che deve tenere conto sia della prerogativa contrattuale attribuita all'imprenditore per la tutela della propria posizione creditoria, sia dei profili extracontrattuali finalizzati alla tutela dei terzi, dipendenti e non.

Si pensi all'impostazione originariamente presente sul codice civile.

L'art. 2049 c.c. si giustificava sul presupposto che il comportamento dannoso del lavoratore subordinato fosse il risultato del mancato controllo dell'imprenditore, tenuto pertanto a rispondere patrimonialmente a fronte di una *culpa in vigilando*.

Oggi il potere di controllo a distanza, di cui è espressione l'art. 4, è divenuto il potere di controllo informatico, il quale ha acquisito una rilevanza del tutto assorbente rispetto ad ogni altra modalità di controllo strumentale.

Si è passati da un metodo orwelliano di controllo, insidioso ma abbastanza semplice da prevedere e contrastare, basato sul sistema dell' "occhio che guarda" (un centro che controlla in tempo reale, grazie a telecamere spesso posizionate in luoghi segreti al fine di realizzare una sorveglianza occulta), ad un controllo più complesso e pervasivo, frammentato, decentralizzato, capillare[23].

Anche qui sarebbe da interrogarsi sulle ragioni che hanno permesso di giustificare l'avvento e dunque la normalità di questa modalità di controllo.

La tecnologia è stata il mezzo, nuovo, creato dall'uomo per soddisfare finalità che a ben vedere di nuovo hanno poco.

Si pensi al binomio filosofico della libertà e sicurezza, due concetti che testimoniano il risalente interrogarsi su come conciliare il dispiegarsi della libertà e dell'autonomia dell'individuo con la necessità di una struttura (lo Stato) che si elevi a garanzia della sicurezza collettiva[24].

---

22 A. PERULLI, il quale sottolinea come il controllo strumentale sia potenzialmente capace di annullare quei frammenti di "mondo vitale" così importanti nella fenomenologia sociale del lavoro e di indurre il lavoratore ad uno sforzo di prestazione stressante e quindi particolarmente lesivo della sua stessa integrità psicofisica tutelata dall'art. 2087 c.c. In *Il potere direttivo dell'imprenditore*, Giuffrè, Milano, 1992, 284.

23 G. ZICCARDI, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, *Labour&Law Issues*, vol. 2, n. 1, 2016, 49.

24 "Io autorizzo e cedo il mio diritto di governare me stesso a quest'uomo o a questa assemblea di uomini, a questa condizione, che tu gli ceda il tuo diritto, e autorizzi tutte le sue azioni in maniera simile. Fatto ciò, la moltitudine così unita in una persona viene chiamata uno stato, in latino *civitas*. Questa è la generazione di quel grande Leviatano o piuttosto - per parlare con più riverenza - di quel Dio mortale, al quale noi dobbiamo, sotto il Dio immortale, la nostra pace e la nostra difesa". T. HOBBES, *Leviatano* (1651), BUR Rizzoli, Milano, 2011, 181-182.

Interrogazione che non perde di attualità, laddove si considerino, con un salto temporale fino ai giorni nostri, le recenti vicende degli attacchi terroristici in occidente.
In una lotta ad un nemico che ormai utilizza con destrezza il mezzo tecnologico, la risposta sembra non potersi porre che sullo stesso piano, fino ad ipotizzare l'estrema conseguenza di un'abdicazione da parte dello Stato democratico ai suoi fondamenti e alle libertà costituzionali, in vista di una legittimazione e quindi giustificazione di un controllo sulla comunità e sull'individuo da parte dei pubblici poteri.
In queste vicende resta ineludibile la ricerca e determinazione del punto di equilibrio tra il ripristino di un'accettabile livello di sicurezza e le garanzie di libertà delle persone[25].
Non c'è dubbio che la situazione che stiamo vivendo richieda maggiore efficacia investigativa, preventiva e repressiva e che in qualche misura ne derivi la compressione di talune libertà.
Ma non bisogna perdere di vista ciò che a livello percettivo iniziamo a ritenere sempre più giustificabile, come appunto un certo tipo di controllo pervasivo.
In conclusione, si può solo ipotizzare che queste più o meno definite ragioni abbiano potuto, da un punto di vista sociologico-metagiuridico, influenzare la scelta del Legislatore, il quale probabilmente si è trovato ad essere assuefatto da una realtà nella quale il significato e la percezione del controllo è radicalmente cambiata.

3. Installazione degli strumenti di controllo ed impiego degli stessi: una distinzione prima non presente. Differenza terminologica tra installazione/impiego.

L'attuale primo comma ha introdotto una distinzione terminologica assente nel vecchio testo normativo.
Il riferimento è ai termini considerati in relazione agli strumenti di controllo, ossia i termini "*impiegati*" ed "*installati*".
Si mette in evidenza che oggi il primo comma dell'art. 4 prevede che gli impianti "possono essere *installati*" previo accordo o autorizzazione e "possono essere *impiegati* esclusivamente" per le esigenze tipizzate dalla legge. Mentre invece la vecchia formulazione della norma, premesso espressamente il divieto di utilizzo degli impianti per finalità di controllo a distanza dell'attività dei lavoratori, richiedeva la sussistenza di esigenze aziendali qualificate per l'autorizzazione all'installazione[26].

25 V. ZAGREBELSKY, *L'equilibrio tra libertà e sicurezza*, in La Stampa del 17 novembre 2015.

26 Comma 2 dell'art. 4 nella formulazione anteriore alla riforma: "Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative, e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le

Alcuni Autori ritengono che la distinzione lessicale non sia frutto di una precisa scelta legislativa.
Si pensi ad Alvino, il quale ritiene che all'impiego dei verbi "*installare*" ed "*impiegare*" non consegue una diversificazione delle condizioni per l'*installazione* e per l'*impiego* dello strumento di controllo. Secondo l'Autore, nel nuovo art. 4 sono definite le condizioni per la legittima installazione dello strumento di controllo e queste condizioni è precisato che valgano per determinate esigenze, che sono quelle tipizzate dalla norma (esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale). Ciò significa che la finalità dell'impiego (quindi le esigenze tipizzate) è condizione per l'installazione dello strumento[27].
Pur non ritenendo sicuro che tale distinzione possa essere ricondotta ad una precisa e ponderata scelta legislativa, si può comunque ipotizzare che la differenza nella formulazione del testo abbia un senso, il quale debba essere ricercato nel fatto che l'impiego degli strumenti di controllo (per finalità inerenti al rapporto di lavoro, quindi con riferimento all'utilizzazione dei dati registrati dagli strumenti, di cui tratta il nuovo comma terzo), purchè legittimamente installati, sia subordinato alle esigenze aziendali tipizzate, laddove invece la condizione legittimante per l'installazione di tali strumenti sia costituita (solo) dall'accordo o autorizzazione[28].
Di conseguenza bisogna ritenere che non sempre l'installazione degli strumenti sia seguita dall'utilizzo degli stessi, considerando che le esigenze aziendali di cui al secondo comma potrebbero non verificarsi.
Tuttavia, anche nel caso in cui non si faccia effettivamente uso di tali strumenti di controllo, è comunque necessario che venga raggiunto l'accordo sindacale (o sia pronunciato il provvedimento autorizzativo) prodromico alla loro installazione.
Questa lettura è in sintonia con una pronuncia della Suprema Corte, la quale ha ritenuto che l'accordo sindacale è sempre necessario anche qualora gli strumenti di controllo non vengano mai utilizzati a tali fini, dopo essere stati installati[29].

---

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."

27 I. ALVINO, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, LLI, vol.2, n. 1, 2016, 15.

28 L. A. COSATTINI *Le modifiche all'art. 4 Stat. Lav. Sui controlli a distanza, tanto rumore; per nulla?*, Lav. nella giur., 11/2015, 985 ss.

29 In tal senso si è pronunciata la Cassazione nella sentenza n. 1490 del 6 Marzo 1986, nella quale si aggiunge che il mancato utilizzo dei sistemi di controllo, installati senza autorizzazione, è utile solo ad evitare al datore di lavoro le sanzioni previste dall'articolo 38 Stat. Lav., e non esclude l'illiceità della semplice installazione; in *Dir. del lav*., II, 83. Della stessa opinione è R. DEL PUNTA, il quale ritiene che la semplice installazione, eseguita in mancanza di accordo

Il cambio di impostazione della norma si spiega con la ormai esplicitata commistione tra diritto del lavoro e diritto della *privacy* e con la tendenza di quest'ultimo a concentrare l'attenzione sulla finalità del trattamento e quindi sulla disciplina che dovrebbe regolarizzare l'utilizzazione delle informazioni registrate dagli strumenti di controllo.

Tale cambiamento consiste nell'aver spostato l'accertamento dell'esistenza di una delle esigenze aziendali qualificate dall'installazione all'impiego dello strumento (accertamento che prima si compiva al fine di verificare la legittima installazione dello strumento e che ora diviene accertamento sulle finalità che giustificano l'impiego dello stesso ai fini del controllo, altrimenti vietato).

Così inteso, non si ritiene che il suddetto cambiamento abbia una rilevanza meramente estetica[30].

Infatti nella nuova formulazione del primo comma emerge chiaramente che l'autorizzazione attiene all'installazione di un impianto che, una volta legittimato, può essere impiegato "esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale".

Da ciò si deduce che tali esigenze si pongono quali finalità esclusive, previste dalla legge, giustificanti le modalità di impiego dello strumento di controllo e quindi anche delle modalità di utilizzazione delle informazioni tramite lo stesso raccolte.

Spetta poi eventualmente al provvedimento di autorizzazione selezionare quali tra le suddette finalità giustifichino il controllo attuato dall'impianto.

Concretizzando, un impianto autorizzato senza indicazione di alcuna specifica finalità potrà essere impiegato per tutti gli scopi previsti dalla legge (esigenze organizzative, sicurezza del lavoro, tutela del patrimonio aziendale), mentre un impianto autorizzato, ad esempio, solo per ragioni di sicurezza sul lavoro potrà consentire l'utilizzo dei dati registrati solo per finalità di tutela dell'integrità del dipendente e non anche per altri scopi.

4. Tutela del patrimonio aziendale e controlli difensivi.

---

sindacale, costituisce di per sé un illecito al di là del successivo utilizzo dell'impianto. *La nuova disciplina dei controlli a distanza sul lavoro (art.23, D. lgs. n. 151/2015), Riv. ita. dir. lav*., 2016, 77 ss.

30 M. MARAZZA ritiene che il cambio di impostazione della norma sia da spiegare con la rinvigorita commistione tra diritto del lavoro e diritto della *privacy* e con la tendenza di quest'ultimo a ricondurre l'attenzione, e quindi la verifica sulla legittimità del controllo, sulla finalità del trattamento. In *Dei poteri (del datore di lavoro), dei controlli (a distanza)e del trattamento dei dati (del lavoratore),*WP CSDLE "Massimo D'Antona". IT- 300/2016, 2016, 14.

Un'altra novità apportata dalla riforma del 2015 è rinvenibile nell'individuazione delle esigenze che legittimano l'impiego degli strumenti di controllo; novità di rilievo sotanziale se non addirittura "epocale"[31]

Il nuovo testo del primo comma include espressamente tra tali esigenze quella relativa alla *tutela del patrimonio aziendale*, mentre l'art. 4, all'originario comma secondo, limitava l'ambito delle esigenze tipizzate, legittimanti il controllo, a quelle organizzative o produttive ovvero a quelle riconducibili alla necessità di garantire la sicurezza sul lavoro.

In questo modo i controlli finalizzati alla tutela del patrimonio aziendale sono stati ricondotti tra quelli che richiedono la procedura autorizzativa disciplinata dal nuovo comma primo, escludendo, in modo ineludibile, che l'installazione di strumenti, finalizzati a tale controllo, sia possibile senza il rispetto della suddetta procedura.

Sul piano generale, deve ritenersi ampliato l'ambito applicativo dei controlli a distanza, a ragione della inclusione della nuova esigenza legittimante detti controlli.

Ora si dovrà tenere conto anche di tutte quelle condotte suscettibili di determinare effetti pregiudizievoli, oltre che sui singoli beni aziendali, anche sulla stessa credibilità ed affidabilità dell'impresa, le quali incidono in misura non certo trascurabile, in termini economici, sul suo patrimonio[32]. Infatti, all'interno della nozione di "patrimonio aziendale" deve essere ricompreso qualsiasi bene, di proprietà dell'azienda, necessario alla produzione, sia esso materiale o immateriale[33].

Il suddetto ampliamento delle finalità di controllo degli strumenti ad esso addetti sembrerebbe dare un senso concreto all'eliminazione del divieto di utilizzare gli impianti al fine di controllare l'attività dei lavoratori, avvenuto con l'abrogazione del vecchio primo comma dell'art.4[34].

---

31 L. A. COSATTINI, *Le modifiche dell'art. 4 Stat. Lav. sui controlli a distanza, tanto rumore; per nulla?*, Il Lav. nella giur., 11/2015, 985 ss.

32 In giurisprudenza è da tempo riconosciuto il diritto al risarcimento dei danni derivanti dalle lesioni all'immagine dei soggetti giuridici. Sulla questione Cass. 1° ottobre 2013, n. 22396, secondo cui nei confronti delle persone giuridiche ed in genere degli enti collettivi è configurabile il risarcimento dei danni non patrimoniali se il fatto lesivo incide su situazioni giuridiche di detti soggetti, che siano equivalenti ai diritti fondamentali della persona umana costituzionalmente protetti, qual è il diritto all'immagine. Lesione tale da determinare una diminuzione della considerazione dell'ente o della persona giuridica da parte dei consociati in genere, ovvero di settori o categorie di essi, con le quali di norma i soggetti lesi interagiscano. Più di recente, Cass. 16 novembre 2015, n. 23401.

33 Cass., sez. lav., sentenza 23 febbraio 2012, n. 2722.

34 M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona". IT – 300/2016, 2016, 16.

E' possibile considerare che anche il puntuale adempimento dell'obbligazione lavorativa concorre alla valorizzazione del patrimonio aziendale, se si considera il diritto di credito dell'imprenditore ad una prestazione di lavoro, che ha indubbiamente un contenuto patrimoniale.
Seguendo tale ragionamento, almeno in linea teorica, ne deriverebbe che il controllo sul lavoro potrebbe giustificare, esso stesso, l'installazione e l'utilizzo dell'impianto.
Ciò significa che all'interno dell'esigenza di tutela del patrimonio aziendale venga ricompresa quella di accertare il corretto adempimento della prestazione lavorativa, di cui è creditore l'imprenditore.
Sempre ricordando, per quanto riguarda il contemperamento delle legittime esigenze delle parti, che gli impianti di cui al primo comma devono essere, innanzitutto, autorizzati in via negoziale o amministrativa ed, inoltre, che le informazioni raccolte potranno essere utilizzate ai fini del rapporto di lavoro solo nel rispetto di quanto previsto dall'attuale terzo comma, e sempre ammesso che l'atto di autorizzazione dell'impianto, negoziale o amministrativo, non contenga al suo interno limiti specifici per ciò che attiene questa specifica modalità di utilizzo (limiti che possono essere posti, ad esempio, nel caso in cui l'autorizzazione sia concessa per finalità diverse da quella della tutela del patrimonio aziendale o sia rilasciata per la tutela del patrimonio aziendale con restrizioni di utilizzo ai fini disciplinari).
La giurisprudenza precedente la riforma aveva disciplinato in modo diverso il controllo effettuato dal datore di lavoro che fosse interessato alla tutela del patrimonio aziendale, creando, nel vuoto normativo, la categoria dei c.d. controlli difensivi.
Infatti questo tipo di controllo non ha ad oggetto le prestazioni dei lavoratori e la loro conformazione alle indicazioni che hanno ricevuto dal datore di lavoro, bensì i comportamenti illeciti, estranei al normale svolgimento della prestazione, anche se da essa occasionati, diretti a ledere il patrimonio aziendale.
Il datore non è quindi interessato al controllo sull'attività lavorativa, quanto piuttosto alle condotte dei lavoratori che siano idonee a ledere la sua proprietà, costituita sia dai beni materiali che compongono l'azienda, sia dai beni immateriali.
Le interpretazioni, giurisprudenziali e dottrinali, inerenti a tali controlli sono state, nel corso del tempo, oscillanti e non univoche, andando a contrapporre in particolare due diversi orientamenti, determinati a seconda dell'inclusione o meno dei controlli difensivi nell'ambito di applicazione dell'art. 4.
La giurisprudenza di legittimità ha definito i controlli difensivi i controlli diretti ad accertare eventuali condotte illecite del lavoratore[35].

35 Cfr. da ultimo Cass. 4 aprile 2012, n. 5371 e Cass. 23 febbraio 2012, n. 2722, entrambe in *Riv. it. Dir. Lav*., 2013, II, con nota di G. SPINELLI.

A partire da un'importante sentenza del 2002[36], la Cassazione ha affermato la totale esclusione dall'ambito di applicazione dell'art.4 delle forme di controllo dirette ad accertare condotte illecite del lavoratore.

In questo modo, i giudici di legittimità, per diverso tempo, hanno ribadito che l'art. 4 ha solo la funzione di accertare condotte illecite del dipendente che si siano consumate nell'orario e sul luogo di lavoro, basandosi sul fatto che i controlli difensivi hanno un oggetto diverso dall'attività lavorativa, cioè svolta dal lavoratore nell'adempimento della sua obbligazione.

Veniva così posta una distinzione basata sull'oggetto del controllo, essendo quest'ultimo permesso senza alcuna autorizzazione nel caso in cui fosse indirizzato alla prevenzione di illeciti commessi da dipendenti o anche da terzi, mentre invece rimaneva nel perimetro della norma statutaria quel controllo che ha sì ad oggetto gli illeciti commessi dal dipendente, purchè riguardanti l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro (e non quando riguardino la tutela di beni estranei al rapporto stesso).

Ne consegue che esula dal campo di applicazione della norma il caso in cui il datore abbia posto in essere verifiche dirette ad accertare comportamenti illeciti del prestatore e lesivi dell'immagine aziendale[37].

La spinta maggiore all'orientamento che vede il controllo difensivo non rientrante nell'applicazione dell'art. 4 era stata data soprattutto dalla giurisprudenza penale, per la quale i suddetti controlli erano sempre leciti quando finalizzati a prevenire o ad accertare il compimento di atti illeciti.

Inoltre stabiliva la piena utilizzabilità delle prove raccolte attraverso i controlli giustificati da motivi difensivi per tutelare il patrimonio aziendale da attività delittuose, da chiunque commesse[38].

---

36 Cass., sez. lav., sentenza 3 aprile 2002, n. 4746.

37 Nella giurisprudenza di merito, App. Roma 23 maggio 2015, in *Il Lav. nella giur.*, 11/2015, 855.

38 Cass. Pen., sez. V, 18 marzo 2010, n. 20722, relativamente ai controlli effettuati attraverso telecamere installate all'interno dei luoghi di lavoro, a beneficio del patrimonio aziendale messo a rischio da possibili comportamenti infedeli dei dipendenti. Si ritengono utilizzabili nel processo penale instaurato contro il dipendente anche i risultati delle videoriprese effettuate all'interno dell'azienda, dovendo detti controlli reputarsi difensivi e come tali consentiti dal disposto dell'art. 4, nota di P. TULLINI, *Videosorveglianza a scopi difensivi e utilizzo delle prove del reato comune del dipendente*, in *Riv. it. Dir. Lav.*, vol. 2, 2011, 85. Ancora, Cass. Pen. 12 luglio 2011, n. 34842, per la quale sono utilizzabili nel procedimento penale, ancorchè imputato sia il lavoratore, i risultati delle riprese video effettuate con telecamere installate all'interno dei luoghi di lavoro ad opera del datore al fine di esercitare un controllo a beneficio del patrimonio aziendale messo a rischio da possibili comportamenti illeciti dei dipendenti. I controlli difensivi sono dunque riconosciuti nei seguenti termini: "ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4, è necessario che il controllo riguardi, direttamente o indirettamente, l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma i controlli difensivi diretti ad accertare condotte illecite del lavoratore".

Tuttavia, con alcune recenti sentenze, si è verificato un cambio di orientamento, attraverso il quale si afferma una posizione più moderata, secondo cui non sarebbe più possibile espungere *tout court* la categoria dei controlli difensivi dalla fattispecie astratta prevista dal secondo comma (precedente disciplina) dell'art. 4.

Ciò è dovuto al fatto per il quale 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[39].

Cambiamento espressamente riconosciuto dalla Cassazione nella sentenza del 1° ottobre 2012, n. 16622, per la quale l'effettività del controllo a distanza dell'attività dei lavoratori richiede che anche per i controlli difensivi trovino applicazione le garanzie dell'art. 4, comma secondo (precedente disciplina), affinchè questi ultimi, così come le altre fattispecie di controllo ivi previste, non si traducano in forme surrettizie di controllo a distanza dell'attività lavorativa. Questa impostazione però sembra cancellare la categoria dei controlli difensivi, dal momento che in questo modo non sarebbero altro che controlli sull'attività lavorativa, vietata o giustificata da altre esigenze.

Infine, si possono considerare, quali fatti indicativi dell'orientamento giurisprudenziale non univoco, due recenti sentenze emanate dai giudici di legittimità.

La sentenza della Cassazione del 27 maggio 2015, n. 10955, che è stata pronunciata con riferimento alla particolare fattispecie della creazione da parte del datore di lavoro di un falso profilo su Facebook con lo scopo di contattare il dipendente al fine di riscontrare l'utilizzo del computer durante l'orario di lavoro per interessi personali. La Corte ha ritenuto legittimi i controlli difensivi occulti se diretti a tutelare beni del patrimonio aziendale, ovvero ad accertare la perpetrazione di comportamenti illeciti, sempre che ciò avvenga mediante modalità non eccessivamente invasive e rispettose della libertà e dignità dei lavoratori e con l'osservanza dei canoni generali di correttezza e buona fede. L'oggetto dell'attività di controllo posta in essere dal datore di lavoro si ribadisce essere un'attività di controllo che non ha avuto ad oggetto l'attività lavorativa e il suo esatto adempimento, ma l'eventuale perpetrazione di comportamenti illeciti da parte del dipendente, poi effettivamente riscontrati e già manifestatisi nei giorni precedenti. Si tratta dunque di un controllo difensivo non solo volto a prevenire e sanzionare un a condotta idonea a ledere il patrimonio aziendale, ma anche un controllo effettuato ex post, in quanto sollecitato dagli episodi dei giorni precedenti, quando il lavoratore aveva violato le disposizioni aziendali che vietano l'uso del telefono cellulare e lo svolgimento di attività extralavorative durante l'orario di lavoro.

L'altra sentenza è quella del 8 novembre 2016, n. 22662, concernente un caso di riprese video di una dipendente, colta nell'atto di sottrarre una busta contenente denaro dalla cassaforte aziendale. Qui la Cassazione ha affermato che le garanzie procedurali imposte dall'art. 4 trovano applicazione

39 Cass., sez. lav., sentenza 17 luglio 2007, n. 15892.

ai controlli difensivi, diretti ad accertare comportamenti illeciti dei lavoratori, quando, però, tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, e non, invece, quando riguardino la tutela di beni estranei al rapporto stesso. Ne consegue che esula dal campo di applicazione della norma il caso in cui il datore abbia posto in essere verifiche dirette ad accertare comportamenti del prestatore illeciti e lesivi del patrimonio e dell'immagine aziendale. La Corte conclude quindi affermando che, nel caso in esame, la condotta della lavoratrice oggetto della ripresa video non solo non atteneva alla prestazione lavorativa ma non differiva in alcun modo da quella illecita posta in essere da un qualsiasi soggetto estraneo all'organizzazione del lavoro. Il c.d. controllo difensivo, pertanto, non atteneva all'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la stessa sicurezza dei lavoratori, oltre al patrimonio aziendale, determinando la diretta implicazione del diritto del datore di lavoro di tutelare la propria azienda mediante gli strumenti connessi all'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale.

Queste sentenze confermano l'esclusione dei controlli difensivi dall'ambito di applicazione del vecchio art. 4 solo se finalizzzati ad accertare comportamenti illeciti dei lavoratori lesivi di beni estranei al rapporto di lavoro.

Una considerazione può essere fatta relativamente a quest'ultimo orientamento giurisprudenziale, inerente al controllo difensivo, che lo ritiene appunto escluso dal campo di applicazione dell'art. 4, proprio perchè esercitato a tutela del patrimonio aziendale, esigenza prima non normata, se pur con riferimento a comportamenti del lavoratore qualificabili come illeciti extracontrattuali e, quindi, non inadempimenti contrattuali.

È fatto notare che si rischia, in questa maniera, di arrivare ad un'interpretazione assai restrittiva, potenzialmente capace di far utilizzare, a fini disciplinari, dati ottenuti attraverso l'impiego dello strumento di controllo, dai quali si evinca un'illecito del dipendente (es. furto), solo se tale strumento fosse stato installato previa autorizzazione ai sensi del primo comma[40].

Da qui, si pone necessaria la ridefinizione del concetto di controllo difensivo, data l'eccessiva limitazione che introdurrebbe ai poteri di controllo del datore di lavoro[41].

---

40 M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore),* WP CSDLE "Massimo D'Antona". IT – 300/2016, 2016, 18.

41 Infatti si può parlare di controllo difensivo in senso stretto laddove mirato ad accertare selettivamente condotte illecite, anche di aggressione al patrimonio aziendale, in base ad indizi concreti, del quale siano autori uno o più dipendenti, anche qualora ciò avvenga in occasione dello svolgimento dell'attività lavorativa. Questi controlli così si collocano al di fuori dell'ambito applicativo dell'art. 4, non avendo ad oggetto l'attività del lavoratore propriamente intesa. A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in AA. VV., *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, Torino, 2017, 10.

Il controllo difensivo dovrebbe, dunque, essere considerato legittimo, anche in mancanza di autorizzazione negoziale o amministrativa, se effettuato mediante impianti il cui utilizzo è orientato a scongiurare il rischio concreto di comportamenti del lavoratore aventi rilevanza penale, posti in essere in occasione dello svolgimento della prestazione lavorativa.
Viene assunto anche il requisito della proporzionalità, in un'ottica secondo la quale il controllo possa essere esclusivamente finalizzato ad accertare lo stato dei fatti a fronte del concreto sospetto di un comportamento illecito[42], per il tempo a ciò strettamente necessario.
La rilevanza penale della condotta posta in essere dal dipendente[43] diviene, dunque, la condizione per individuare una categoria aggiornata di controlli difensivi, i quali trovano appunto la loro giustificazione nella rilevazione della condotta illecita del dipendente e non più nell'esigenza di tutela del patrimonio aziendale.
In questo modo tali controlli esulano dall'ambito di applicazione dell'art. 4, non necessitando, gli strumenti di controllo, della procedura autorizzativa di cui al primo comma.

4.1 Legittimità dei controlli occulti.

Nel discutere sulla categoria dei controlli difensivi ci si imbatte nella specifica tipologia dei controlli occulti, operati eventualmente dal datore di lavoro.
Si diceva, nel precedente paragrafo, che la giurisprudenza è giunta ad affermare che i controlli difensivi, diretti ad accertare comportamenti illeciti dei lavoratori, sono soggetti alle garanzie procedurali di cui all'art. 4, ma ciò solo nel caso in cui tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, e non, invece, quando riguardino la tutela di beni estranei al rapporto stesso.
In questo modo, era stato aperto il varco ad un ampia "zona franca" ove l'art. 4 fosse ritenuto inapplicabile qualora il controllo avesse avuto, quale obiettivo primario, quello di tutelare il patrimonio aziendale nei confronti di comportamenti illeciti messi eventualmente in atto dai dipendenti.
Controllo il quale poteva essere effettuato anche con modalità occulte. Si ricorda che, con la modifica normativa, il Legislatore ha espressamente ricondotto i controlli finalizzati alla tutela del patrimonio aziendale fra quelli tipizzati dall'art. 4, prevedendo, quale presupposto per la loro legittimità, il previo esperimento della procedura amministrativa, disciplinata dal nuovo primo

42 Relativamente al sospetto di un illecito compiuto o della mera ipotesi del suo compimento, Cass., sez. lav., n. 3590/2011; Cass., sez. lav., n. 13789/2011.

43 Si pensi a qualche esempio: furto (art. 624 c.p.), truffa (art. 640 c.p.), danneggiamento (art. 635 c.p.), lesioni personali dolose (art. 582 c.p.), lesioni personali colpose (art. 590 c.p.).

comma. Così facendo, l'unica tipologia di controllo difensivo ammissibile, senza la previa autorizzazione, sarà quello diretto ad accertare la commissione di un illecito da parte del lavoratore, sia nel caso in cui la condotta antigiuridica sia già stata posta in essere, sia nel caso sussistano gravi indizi a suo carico. Ciò sempre qualora il comportamento illecito riguardi beni estranei al rapporto di lavoro e cioè non possa essere ricondotto ad un inadempimento contrattuale.

Il controllo occulto è un tipo di controllo effetuato nei confronti dei dipendenti dell'impresa, i quali non sono a conoscenza della sua esistenza, essendone sottoposti a loro insaputa.

L'utilità di questa categoria di controlli sorge nel momento in cui il datore di lavoro, al fine di tutelare la propria azienda e il suo patrimonio dall'eventuale attività illecita dei dipendenti, non ha altri mezzi se non i controlli occulti.

Il controllo occulto diretto a controllare unicamente l'attività lavorativa del dipendente è vietato dal primo comma dell'art. 4 (nella versione originaria, in modo esplicito, ora, in seguito alla riforma, implicitamente).

Si pone la questione della liceità dei controlli occulti finalizzati a rispondere alle esigenze di cui all'attuale primo comma.

È qui da considerare che, il controllo occulto, per sua natura, andrebbe a cozzare con una delle due possibilità date dalla procedura, ossia con il prodromico accordo riconosciuto da una contrattazione collettiva (rappresentanza sindacale). Ciò nella convinzione secondo la quale il sindacato tenda a dare sempre ampia pubblicità della propria attività, vanificando così l'intenzione del datore di lavoro di mettere in atto una forma nascosta di controllo.

È stata la giurisprudenza di legittimità a chiarire le cose, riconoscendo esplicitamente la liceità dei suddetti controlli, almeno nei casi in cui il controllo sia deputato ad appurare comportamenti diversi dal mero inadempimento della prestazione lavorativa.

Merita citare la prima pronuncia a riguardo[44], anche se non avente propriamente ad oggetto il controllo a distanza, la quale ha affermato la liceità del controllo occulto quale modalità messa in atto da personale esterno (nel caso specifico, personale di una agenzia investigativa), assunto dall'imprenditore allo scopo di controllare l'adempimento delle prestazioni lavorative e quindi di accertare mancanze specifiche dei dipendenti già commesse o in corso di esecuzione.

Ciò indipendentemente dalle modalità del controllo, che può avvenire anche occultamente, senza che vi ostino né il principio di correttezza e buona fede nell'esecuzione dei rapporti, né il divieto

44 Cass., sez. lav., sentenza 10 luglio 2009, n. 16196, che ha riconosciuto la liceità dei controlli occulti sia nel caso in cui vengano svolti dal datore di lavoro per il tramite della propria organizzazione gerarchica, sia attraverso personale esterno che, nello specifico, era costituito da personale di un'agenzia investigativa. Così successivamente Cass. 4 dicembre 2014, n. 25674.

implicito di cui all'art. 4, riferito esclusivamente all'uso di apparecchiature per il controllo diretto a distanza.

Più recentemente, una conferma circa la liceità del controllo difensivo occulto (non operato per il tramite di personale esterno, bensì attraverso controlli tecnologici più propriamente rientranti nella tipologia di atti di monitoraggio ex art. 4) è stata data dalla già citata sentenza della Cassazione del 27 maggio 2015, n. 10955.

Qui è stata reputata legittima l'attività di controllo posta in essere dal responsabile del personale, a ciò autorizzato dai vertici aziendali, consistita nella creazione di un falso profilo su un *social network* (*Facebook*) al fine di verificare la presenza su tale piattaforma del dipendente durante l'orario di lavoro, in quanto avente ad oggetto non l'attività lavorativa più propriamente detta ed il suo esatto adempimento, bensì l'eventuale perpetrazione di comportamenti illeciti, già manifestati, da parte del dipendente.

Il controllo difensivo occulto, destinato pertanto a riscontrare e a sanzionare un comportamento del prestatore di lavoro idoneo a ledere il patrimonio aziendale, viene esercitato, dunque, *ex post* e sollecitato da episodi già occorsi. Tali sono stati, specificamente, il riscontro della violazione da parte del dipendente della disposizione aziendale che vieta l'uso del telefono cellulare e lo svolgimento di attività extralavorativa durante l'orario di servizio.

Il controllo così messo in atto esula dall'ambito di applicazione dell'art. 4, poiché non ha ad oggetto l'attività lavorativa e il suo esatto adempimento, bensì l'eventuale commissione di illeciti da parte del dipendente, idonei a ledere il patrimonio aziendale, sotto il profilo del regolare funzionamento e della sicurezza degli impianti[45].

Una recente pronuncia della Cassazione[46] ha affermato il divieto di operare un controllo "a sorpresa" da parte del datore di lavoro, realizzato attraverso l'installazione di apparecchi e *software* che consentano un'opera di monitoraggio approfondita sulla posta elettronica, sulle telefonate e sulla navigazione Internet effettuata dal dipendente, senza il previo raggiungimento dell'accordo sindacale o, in mancanza, dell'autorizzazione amministartiva e senza il rilascio delle adeguate informative, ciò in ragione del fatto che i controlli così messi in atto hanno ad oggetto l'adempimento dell'attività lavorativa e non beni estranei al rapporto di lavoro[47].

---

45 La Cassazione ha comunque ribadito come fondamentali i limiti e le garanzie poste a tutela dei lavoratori, imponendo che l'esplicazione delle attività di accertamento sia posta in essere 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 ed alla difesa dell'organizzazione produttiva aziendale deve contemperarsi, in ogni caso sempre secondo i canoni generali della correttezza e buona fede contrattuale. Cass., sez. lav., 27 maggio 2015, n. 10955.

46 Cass. 19 settembre 2016, n. 18302.

47 Già con la sentenza n. 4375 del 23 febbraio 2010, la Cassazione affermava che il controllo operato mediante strumenti informatici sulla posta elettronica e sugli accessi ad Internet fosse da qualificarsi come controllo

5. Accordo sindacale e autorizzazione amministrativa. Modifiche apportate dal d.lg. 185/2016.

Nella formulazione della nuova norma, come in quella precedente la riforma, è prevista, come regola generale, la necessità di un previo accordo sindacale o in mancanza di questo una previa autorizzazione amministrativa[48].

La riforma del 2015 e successivamente una modifica apportata dal d.lgs. 185/2016 hanno innovato la materia relativa alla procedimentalizzazione dell'installazione degli impianti audiovisivi e degli altri strumenti dai quali possa derivare anche un controllo a distanza sull'attività dei lavoratori (installazione consentita solo per le finalità espressamente disciplinate), contenuta nel primo comma dell'art. 4[49].

Ad essere cambiati sono, innanzitutto, i soggetti legittimati alla conclusione dell'accordo, in quanto, in primo luogo, è stabilito che alla sua negoziazione sono legittimate sia le rappresentanze sindacali aziendali che le rappresentanze sindacali unitarie[50].

---

preterintenzionale (rientrante nella procedura dell'allora comma 2 dell'art. 4). Inoltre aveva dichiarato che "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, l'attività lavorativa e se la stessa sia svolta in termini di diligenza e di corretto adempimento".

48 Nuovo comma 1: "Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale 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. Comma così modificato dall'art. 5, comma 2, d.lgs. 24 settembre 2016, n. 185, a decorrere dall'8 ottobre 2016, ai sensi di quanto disposto dall'art. 6, comma 1, del medesimo d.lgs. n. 185/2016.

49 Quanto alla finalità espletata da tale onere procedurale, può richiamarsi P. ICHINO, secondo cui questo strumento della "procedimentalizzazione" dell'esercizio del potere imprenditoriale sia stato utilizzato dal Legislatore come strumento di tutela dei diritti del lavoratore. Infatti, la norma non può essere letta come tendente ad indebolire la protezione del lavoratore, rendendola disponibile in sede di negoziazione collettiva aziendale, ma piuttosto deve essere letta come tendente a rafforzare tale protezione, in quanto l'accordo collettivo preventivo determina proprio l'*an* e il *quomodo* dell'installazione dello strumento. In *Il contratto di lavoro*, Vol. 3, Giuffrè, Milano, 2003, 231.

50 Il testo precedente menzionava invece solo le RSA ovvero, in mancanza di esse, la commissione interna, che aveva suscitato dubbi sulla legittimazione delle RSU a negoziare l'accordo. In passato sia la Cassazione che il Ministero del lavoro si erano espressi nel senso dell'impossibilità di sostituire la titolarità delle RSA, a ricercare un preventivo accordo con l'azienda ai sensi dell'art. 4, con quella di organismi diversi; Cass., sez. lav., 16 settembre 1997, n. 9211;

In secondo luogo, la norma si arricchisce con la previsione dell'ipotesi delle imprese multilocalizzate (imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni), nel cui caso l'accordo potrà essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale.

È da ritenere che anche la nuova norma ponga in capo al datore di lavoro un obbligo a trattare con le rappresentanze sindacali, la cui violazione può essere fatta rientrare nell'ambito di tutela previsto dall'art. 28 Stat. Lav. ed il cui fallimento è condizione per poter inoltrare la richiesta di autorizzazione in via amministrativa. Si può interpretare il fatto che l'autorizzazione amministrativa possa essere richiesta e concessa solo in mancanza di accordo come una condizione che può ritenersi verificata solo in quanto sia stata avviata la trattativa e questa si sia conclusa per l'impossibilità di stipulare un contratto collettivo. A conferma di tale conclusione sta il fatto che l'accordo, da stipularsi con le accociazioni sindacali comparativamente più rappresentative sul piano nazionale, nell'ipotesi di imprese multilocalizzate, venga espressamente posto quale alternativa. In questo senso l'avvio di una trattativa sindacale è qualificata come onere, con la conseguenza che al datore di lavoro resterebbe inibita la possibilità di chiederne l'intervento ministeriale se non in caso di fallimentodel tentativo.

La giurisprudenza ritiene antisindacale il comportamento del datore di lavoro che proceda ad installare un impianto, atto al controllo a distanza, senza preventivamente aver tentato di raggiungere un accordo con le rappresentanze dei lavoratori (così a partire da Cass., sez. lav., 16 novembre 1997, n. 9211).

Ministero del lavoro nota del 19 giugno 1989. Secondo M. PERSIANI si tratta di un accordo destinato, inevitabilmente, a produrre effetti nei confronti di tutti i dipendenti occupati nell'unità produttiva, quindi indipendentemente dall'iscrizione o dall'affiliazione alla struttura sindacale nel cui ambito le rappresentanze sindacali sono state costituite. In *Diritto sindacale*, sedicesima edizione, Cedam, Padova, 2015. Cass. Pen., Sez. III, 17 aprile 2012, n. 22611, ha ritenuto che l'installazione nel luogo di lavoro di un sistema di videosorveglianza mediante telecamere non costituisce reato, ai sensi del combinato disposto degli art. 4 e 38 l. 300/70, laddove, pur in assenza di autorizzazione sindacale, risulti comprovato l'assenso all'installazione da parte della totalità dei lavoratori dell'azienda, poiché non può essere negata validità ad un consenso chiaro ed espresso proveniente da tutti i lavoratori e non soltanto da una loro rappresentanza. Per contro Cass., Sez. Lav., 10 ottobre 2012, n. 16622. Tale orientamento giurisprudenziale è stato totalmente ribaltato dalla sentenza della Cass. Pen., sez. III, 8 maggio 2017, n. 22148, la quale sottolinea, invece, la necessità dell'interlocuzione con le rappresentanze sindacali, al fine di tutelare interessi di carattere collettivo, di cui il lavoratore non può disporre, che altrimenti verrebbero lesi. La Corte infatti afferma che, anche a seguito delle modifiche apportate dalla riforma, non possa avere "alcuna rilevanza il consenso scritto o orale concesso dai singoli lavoratori, in quanto la tutela penale è apprestata per la salvaguardia di interessi collettivi di cui, nel caso di specie, le rappresentanze sindacali, per espressa disposizione di legge, sono portatrici, in luogo dei lavoratori che, a causa della posizione di svantaggio nella quale versano rispetto al datore di lavoro, potrebbero rendere un consenso viziato".

Ai fini della validità dell'accordo, occorre determinare la regola di formazione della volontà della rappresentanza, fattore non esplicitato dalla norma.

Con riferimento all'ipotesi in cui in azienda sia costituita una RSU, varrà la regola maggioritaria, in quanto prevista espressamente dall'accordo istitutivo delle RSU (art. 7 del Testo Unico sulla Rappresentanza del 10 gennaio 2014[51]), quindi l'apparecchiatura potrà dirsi validamente installata solo se autorizzata all'interno di un contratto collettivo approvato dalla maggioranza dei componenti della RSU. Ciò in ragione del fatto che il riferimento all'organo di origine pattizia per la stipulazione dell'accordo ai fini dell'installazione comporta il rinvio alle regole dettate dall'accordo istitutivo dell'organo stesso.

Per quanto riguarda l'ipotesi in cui in azienda siano costituite delle RSA, si può fare riferimento a due casi.

Nel primo, relativo al caso in cui l'azienda sia tra quelle tenute all'applicazione del Testo Unico del 2014, si potrà invocare la regola dettata nella Parte Terza di quest'ultimo, 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".

Nel secondo caso, quello in cui l'azienda sia fuori dell'ambito di applicazione del Testo Unico, la disposizione non chiarisce se debba valere anche qui la regola maggioritaria o se l'accordo possa ritenersi valido solo se ottenuto con il consenso di tutte le RSA presenti in azienda.

A questo proposito, va ricordata la Risposta ad Interpello del Ministero del Lavoro[52], con la quale il Ministero si era espresso a favore della regola maggioritaria, secondo cui, per la legittimità dell'accordo, occorre la sua sottoscrizione ad opera della sola maggioranza delle RSA o, meglio, da

51 Il 10 gennaio 2014 è stato siglato l'Accordo Interconfederale tra Cgil, Cisl, Uil e Confindustria in merito al Testo Unico sulla rappresentanza. Questo testo ha avuto origine dall'applicazione degli accordi siglati tra Confindustria e i Sindacati confederali di Cgil, Cisl e Uil il 28 giugno 2011 e del 31 maggio 2013. Questo recepisce e dà attuazione ai contenuti dell' Accordo del 28/6/2011, del Protocollo del 31/5/2013 ed aggiorna i contenuti dell'Accordo sulle RSU del 20/12/1993.

52 Risposta ad Interpello 5 dicembre 2005, prot. 2975. L'Interpello aveva ad oggetto l'istanza avanzata dall'Associazione Bancaria Italiana in materia di controlli a distanza, circa l'individuazione dei requisiti dell'accordo da stipularsi con le RSA. L'ABI aveva richiesto di pronunciarsi sulla legittimità della centralizzazione della procedura sindacale o amministrativa di autorizzazione all'installazione degli impianti di controllo nel luogo ove è ubicata la direzione generale dell'istituto, senza coinvolgere necessariamente le RSA o la DTL delle province dove erano situate le singole unità produttive dell'istituto. Il Ministero ha optato per la legittimità di tale orientamento, sul presupposto che "la necessaria adesione di tutte le RSA finirebbe per tradursi in un vero e proprio diritto di veto utilizzabile anche dalla RSA più esigua, che potrebbe, in tal modo, vanificare l'accordo raggiunto con le altre componenti aziendali".

parte delle RSA che esprimano la maggioranza del personale, senza che sia necessario il consenso unanime di tutte le RSA.

Inoltre, nel medesimo provvedimento, il Ministero aveva chiarito, con riferimento alla possibilità di centralizzare la procedura di cui all'art. 4, che l'accordo con le RSA situate, in quello specifico caso, nel luogo della direzione generale dell'istituto bancario istante, non fosse sufficiente a legittimare l'installazione delle apparecchiature di controllo e ciò nemmeno qualora l'impianto tecnologico presenti caratteristiche costruttive e di funzionamento standardizzate in tutto il territorio. Infatti, secondo il Ministero il coinvolgimento delle RSA "più vicine" troverebbe ragione nella natura dei diritti coinvolti, assolutamente personali, quali il diritto alla riservatezza del lavoratore, i quali esigono, per forza di cose, una tutela più stringente[53].

La nuova disposizione, in funzione decisamente semplificatoria del regime autorizzatorio, ha introdotto una regola specifica per l'ipotesi in cui l'impresa, che intenda installare strumenti di controllo preterintenzionale, sia dotata di unità produttive ubicate in diverse province della stessa regione ovvero in più regioni[54].

Dunque, nell'ipotesi di imprese multilocalizzate, il nuovo primo comma permette, nell'eventualità in cui non sia possibile per l'azienda raggiungere l'accordo sindacale a livello territoriale, che l'accordo possa essere stipulato con l'associazione sindacale comparativamente più rappresentativa sul piano nazionale, senza dover "passare" necessariamente per le RSA.

A seguito dell'ultima modifica apportata dal d.lgs. n. 185 del 24 settembre 2016, l'art. 4 stabilisce che, in mancanza di accordo collettivo, il datore di lavoro, che voglia richiedere l'autorizzazione in via amministrativa, potrà rivolgersi alla sede territoriale dell'Ispettorato Nazionale del Lavoro. Nell'ipotesi in cui si tratti di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, il datore ha la possibilità, in alternativa, di richiedere l'autorizzazione alla sede centrale dell'Ispettorato Nazionale del Lavoro[55].

---

53 Con tale osservazione il Ministero del Lavoro ha fatto proprio un precedente orientamento della Cassazione (Cass., Sez. lav., 16 settembre 1997, n. 9211), secondo cui la tassatività dei soggetti indicati all'art. 4 esclude che possano essere considerati legittimati alla conclusione dell'accordo gli organi di coordinamento delle RSA di varie unità produttive, precisando che, per considerare legittima l'installazione dello strumento di controllo, fosse necessaria la stipulazione di un autonomo accordo sindacale in ciascuna unità produttiva.

54 Si pensi, quali imprese strutturate su più unità produttive multilocalizzate, agli istituti di credito. In questo caso, la nuova disposizione consente che si eviti la necessità di coinvolgere in separate negoziazioni le RSA delle diverse unità produttive interessate, superando così l'interpretazione restrittiva delineata dal Ministero del Lavoro e in precedenza dalla Cassazione.

55 La facoltà attribuita alle imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali dell'Ispettorato Nazionale del Lavoro di richiedere un'unica autorizzazione alla sede centrale dello stesso prospetta, oltre che una semplificazione, anche l'eventualità affinché si formi, presso l'INL, relativamente agli strumenti di

L'intervento correttivo operato dal decreto legislativo del 2016 ha così sostituito il precedente riferimento alle Direzioni territoriali del lavoro e del Ministero del Lavoro[56].

In questo senso c'è un ritorno alla previsione normativa così com'era disposta precedentemente la riforma del Jobs Act, ove si faceva riferimento proprio all'Ispettorato del Lavoro, il quale, in difetto di accordo con le rappresentanze sindacali aziendali, provvedeva, su istanza del datore di lavoro interessato all'installazione degli impianti dai quali potesse derivare un controllo, dettando anche le modalità per l'uso di tali impianti[57].

Si deve ritenere che queste modifiche, relative ai soggetti legittimati a fornire l'autorizzazione amministrativa all'installazione dello strumento di controllo preterintenzionale, non comportino incisive alterazioni della portata sostanziale della norma.

L'ultimo intervento correttivo apportato dal d.lgs. 185/2016 è attinente ai profili di contenzioso amministrativo rispetto ai provvedimenti dell'Ispettorato Nazionale del Lavoro e degli Ispettorati Territoriali del Lavoro. Infatti, si sancisce che l'autorizzazione rilasciata dalla sede territoriale dell'INL o, in alternativa, per le imprese con più unità produttive collocate in più ambiti territoriali, dalla sede centrale dell'INL, sia da considerarsi provvedimento definitivo, tale quindi da non essere suscettibile di ricorso gerarchico amministrativo.

In realtà già la disposizione dell'art. 4, come modificata dal d.lgs. 151/2015 rispetto a quella previgente, non conteneva più l'esplicita previsione di un contenzioso amministrativo avverso l'autorizzazione, essendo stata abrogata la norma che espressamente prevedeva la possibilità di

---

controllo a distanza aventi funzioni identiche o simili, una sorta di giurisprudenza, che con i suoi precedenti, uniformi tra loro data l'unicità del soggetto decisore a livello nazionale, sia suscettibile di condizionare i comportamenti delle imprese, dei sindacati e delle stesse sedi territoriali dell'Ispettorato nella suddetta valutazione sugli strumenti. A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in AA. VV., *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, Torino, 2017, 12.

56 La normativa del primo comma dell'art. 4, conseguente alla riforma attuata con il d.lgs. 151/2015 disponeva: "In mancanza di accordo, gli impianti e gli strumenti di cui al periodo precedente possono essere installati previa autorizzazione della Direzione territoriale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più Direzioni territoriali del lavoro, del Ministero del lavoro e delle politiche sociali".

57 Nel testo originario precedente l'intervento del d.lgs. 151/2015, il secondo comma dell'art. 4 stabiliva: "Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure in mancanza di queste, con la 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".

impugnare, mediante ricorso alla competente Direzione generale del Ministero del Lavoro, le decisioni dell'Ispettorato del Lavoro[58].

Tuttavia, in sede ministeriale, si è ritenuto di sostenere che il provvedimento adottato dalla DTL potesse continuare ad essere ricorribile mediante ricorso gerarchico alla Direzione generale del Ministero e ciò a norma dell'art.1, comma 1, del D.P.R. del 24 novembre 1971, n. 1199, la quale, essendo norma di carattere generale, consente di ricorrere contro il provvedimento amministrativo di autorizzazione o di diniego dell'Ufficio territoriale, dovendosi considerare lo stesso atto "non definitivo"[59].

Attualmente tale possibilità è stata radicalmente esclusa dall'intervento correttivo, anche in ossequio a quanto espressamente specificato nella Relazione illustrativa che correda il provvedimento normativo modificatore, secondo la quale, con la modifica normativa proposta, viene chiarito che i provvedimenti autorizzatori adottati dall'Ispettorato del Lavoro sono definitivi, per cui non è possibile proporre contro gli stessi ricorso gerarchico. Questo deriva proprio dal fatto che i provvedimenti autorizzatori sono adottati tanto dalle sedi territoriali, quanto, a scelta delle imprese multilocalizzate, dalla sede centrale dell'INL. E mentre per i provvedimenti delle sedi territoriali potrebbe ipotizzarsi un ricorso alla sede centrale, nei confronti dei provvedimenti di quest'ultima non è possibile individuare un superiore gerarchico. Infatti il rapporto che lega l'Ispettorato del Lavoro al Ministero del lavoro e delle politiche sociali si qualifica come rapporto di vigilanza e non gerarchico[60].

6. Distinzione tra "strumenti di controllo" e "strumenti di lavoro". L'esempio del GPS.

Emerge macroscopica la differenza tra la disciplina applicabile agli "strumenti di controllo a distanza" (comma 1) e agli "strumenti di lavoro", dai quali comunque derivi un controllo a distanza (comma 2).

---

58 Art. 4, comma quarto, testo precedente la riforma del d.lgs. 151/2015, ora abrogato: "Contro i provvedimenti dell'Ispettorato del lavoro il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna oppure i sindacati dei lavoratori, di cui al successivo art. 19, possono ricorrere, entro trenta giorni dalla comunicazione del provvedimento, al Ministero per il lavoro e la previdenza sociale".

59 Si tratta del D.P.R. sulla semplificazione dei procedimenti in materia di ricorsi amministrativi, il cui art. 1, comma 1, stabilisce: "Contro gli atti amministrativi non definitivi è ammesso ricorso in unica istanza all'organo sovraordinato, per motivi di legittimità e di merito, da parte di chi vi abbia interesse".

60 Relazione illustrativa all'Atto del Governo n. 311/2016, che costituisce lo schema di D.Lgs. adottato dal Consiglio dei Ministri nella seduta del 10 giugno 2016, recante "disposizioni integrative e correttive dei decreti legislativi 15 giugno 2015, n.81 e 14 settembre 2015, nn. 148, 149, 150 e 151", all'esame delle Commissioni competenti di Senato e Camera del 21 giugno 2016.

Solo nel primo caso è richiesta la procedura (negoziale o amministrativa) di autorizzazione all'installazione dello strumento e i controlli possono essere effettuati esclusivamente per le finalità tipizzate dal legislatore (esigenze organizzative e produttive, di sicurezza del lavoro, di tutela del patrimonio aziendale).

Si può considerare lo "strumento di lavoro" come *species* rientrante nel più ampio genere degli "strumenti di controllo"[61].

In entrambi i casi si tratta di strumenti potenzialmente in grado di monitorare a distanza l'attività del lavoratore.

La particolarità del fenomeno del controllo, così come inteso attualmente nel rapporto di lavoro, sta nel fatto che adesso anche lo strumento di lavoro si configura quale strumento di controllo, e non può essere diversamente, dato che determinate tipologie di strumenti di lavoro sono il prodotto dell'evoluzione tecnologica e dell'era informatica e si pongono quali indispensabili mezzi nello svolgimento della prestazione lavorativa, e più in generale della comunicazione e connessione nella società dell'informazione[62].

---

61 Si vuole da subito fare un inciso relativamente al controllo datoriale e agli strumenti di cui si avvale come considerati e regolati dalla contrattazione collettiva di prossimità. L'art. 8 del d.l. n. 138/2011 (convertito in legge dalla l. n. 148/2011) ha considerato tale argomento includendo alla lett. a), co. 2 gli impianti audiovisivi e l'introduzione di nuove tecnologie quali oggetto delle specifiche intese (di cui al co. 1). In questo modo, la contrattazione collettiva di prossimità pare assumere un ampio potere derogatorio (nei confronti della legge e del contratto collettivo nazionale) in materia, tale da introdurre, allargare o ridimensionare la gamma degli strumenti per i quali si rende necessaria la preventiva autorizzazione sindacale o amministrativa. È comunque improbabile che l'accordo collettivo possa introdurre l'installazione di strumenti finalizzati al controllo a distanza dell'attività dei lavoratori o che i controlli possano essere autorizzati in violazione delle norma poste a difesa del diritto di riservatezza dei lavoratori. Così A. TEA, *Controlli a distanza:spunti problematici e sviluppi interpretativi*, *il Lav. nella giur*., vol.1, 2017, 26. E così prima per I. ALVINO, per il quale si esclude necessariamente che l'accordo collettivo possa consentire l'installazione di una tecnologia la cui specifica finalità sia quella di controllare l'attività lavorativa e si deve considerare che i principi della disciplina della *privacy* pongono una resistenza nei confronti dei poteri conferiti all'autonomia negoziale collettiva eventualmente rivolta ad un ridimensionamento della tutela della riservatezza del lavoratore. *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, LLI, vol. 2, n. 1, 2016, 42.

62 Negli ultimi tre decenni si è registrata una rapida innovazione nella tecnologia dell'informazione. La telefonia mobile, Internet e i sistemi di trasmissione digitale ad alta velocità hanno rivoluzionato gran parte del mondo che ci circonda. Volendo brevemente definire la società dell'informazione, con essa si intende l'attuale società post-industriale, nella quale ciò che maggiormente emerge è il prevalere di un bene immateriale, come l'informazione, rispetto all'industria. Oggi l'informatica (apparecchi digitali e programmi *software*) e le telecomunicazioni (comprese le reti telematiche) sono i due pilastri su cui si regge tale società. Dunque, si tratta della società odierna caratterizzata da un'economia basata largamente sulla produzione di servizi, specializzati nella manipolazione delle informazioni, e sul valore economico della conoscenza come risorsa strategica (*know how*, brevetti). Secondo questa visione oggi la società

Da sempre il controllo, attraverso strumenti tecnologici, sia dell'essere umano in generale e sia del lavoratore (sul posto di lavoro o anche fuori dei locali dell'azienda) ha presentato una stretta connessione con l'evoluzione tecnologica.

A partire dagli anni Settanta e poi negli anni Ottanta e Novanta, l'attenzione era rivolta soprattutto nei confronti degli apparecchi telefonici aziendali, delle autovetture di servizio e di ciò che si svolgeva all'interno degli ambienti dell'azienda, ad esempio allestendo pareti di vetro trasparenti, finestre o telecamere. Si trattava di un tipo di controllo "classico", centralizzato, come già accennato in precedenza, di stile orwelliano[63].

Dalla fine degli anni Novanta è comparso il primo cambiamento apportato dalla tecnologia, con risvolti pregnanti nell'ambito della sfera personale del lavoratore, ossia la possibilità per l'impianto non solo di svolgere videoriprese in tempo reale, ma anche di memorizzare i dati per lunghi periodi.

Successivamente, l'avvento dei telefoni cellulari (poi divenuti *smartphone)*, i *personal computer*, i sistemi *software* e la rete Internet hanno stravolto il concetto di controllo nel rapporto di lavoro, annullando il binomio strumento di controllo/strumento di lavoro, in quanto, potenzialmente, uno strumento di lavoro è anche strumento di controllo.

Si realizza così un controllo decentralizzato, frammentato, ove i dati acquisiti sono sia lavorativi che privati, rendendo la separazione tra vita privata e vita lavorativa difficile da determinare, se non impossibile.

La nuova disciplina dell'art. 4 è stata sì riscritta con la consapevolezza della necessità di porre dei limiti a questa tendenza ispettiva e pervasiva suscettibile di realizzarsi in ambito lavorativo in una realtà ove sia lo stesso strumento di lavoro a permettere eventualmente il controllo sulla vita privata, ma anche con la volontà di non imbrigliare in un sistema procedurale autorizzatorio l'interesse del datore di lavoro al controllo sul corretto adempimento della prestazione, quale espressione del suo potere direttivo,

Andando in cerca di una definizione di strumenti di lavoro al fine di individuare una differenza concettuale con gli strumenti di controllo, ci si imbatte proprio nel testo del secondo comma, il quale è esso stesso a definire gli strumenti di lavoro quali "strumenti utilizzati dal lavoratore per

---

fonda i rapporti interpersonali e l'assetto socio-produttivo sull'uso delle tecnologie dell'informazione e della comunicazione, tutto ciò in vista del massimo obiettivo dell'aumento della produttività e competitività del sistema economico.

63 G. ZICCARDI, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, LLI, Vol. 2, n. 1, 2016, 48.

rendere la prestazione lavorativa"[64] ed, inoltre, dispone che a questi non si applichi la disciplina procedurale di cui al primo comma.

Dunque la differenza emerge, innanzitutto, dal punto di vista della finalità con cui lo strumento viene impiegato e per il quale viene introdotto dal datore di lavoro (controllo preterintenzionale, da un lato e prestazione lavorativa, dall'altro). Si fa riferimento al fatto che lo strumento di lavoro è introdotto dal datore di lavoro nell'esercizio del potere di organizzazione del lavoro, al fine di realizzare un suo interesse alla prestazione oggetto del contratto, mentre lo strumento di controllo preterintenzionale è installato nell'esercizio di poteri di organizzazione dell'attività, attribuiti all'imprenditore per soddisfare altre esigenze, non direttamente riportate quali oggetto del contratto, ma comunque funzionali alla realizzazione dello stesso (esigenze organizzative, produttive, di sicurezza del lavoro, di tutela del patrimonio aziendale).

In secondo luogo vi è la differenza dettata dalla norma, relativa alla procedura prodromica all'installazione e all'impiego di una tipologia di strumento e non all'altra.

In merito a tale previsione, da un lato, si considera che l'esclusione del regime autorizzatorio, riservata agli strumenti di lavoro, costituisca una semplificazione, in quanto evita che si verifichino, oltre a ritardi e inefficienze insite a tale sistema procedurale, situazioni paradossali nelle quali il datore di lavoro sarebbe obbligato ad ottenere l'autorizzazione anche per dotare i propri dipendenti di un *personal computer* o di uno *smartphone.*

Dall'altro lato, è anche da considerare che l'esclusione del regime autorizzatorio non significa aver attribuito al datore di lavoro la facoltà di monitorare continuativamente l'attività del lavoratore attraverso l'analisi dei dati registrati. La possibilità di installare lo strumento va, infatti, tenuta distinta dalla possibilità di analizzare le informazioni dallo stesso registrate[65]. Pur non essendo necessaria l'autorizzazione, il datore di lavoro non è libero di controllare ed esaminare i dati

64 Come chiarito con nota ministeriale del 18 giugno 2015, l'espressione "per rendere la prestazione lavorativa" comporta che l'accordo o l'autorizzazione non servono se, e nella misura in cui, lo strumento viene considerato quale mezzo che "serve" al lavoratore per adempiere la prestazione. Tuttavia, come indicato nella nota, nel momento in cui lo "strumento di lavoro" viene modificato (ad esempio, con l'aggiunta di appositi *software* di localizzazione o filtraggio) per controllare il lavoratore, si fuoriesce dall'ambito della disposizione, in quanto, in tal caso, da strumento che "serve" al lavoratore per rendere la prestazione il pc, il *tablet* o lo *smartphone* diventerebbero strumenti che servono al datore per controllarne la prestazione. Il Ministero in questo modo fornisce un'interpretazione assai restrittiva circa la definizione di strumento di lavoro, quasi andando ad ignorare, nella sua specificazione circa la distinzione tra lo strumento e l'eventuale applicativo informatico aggiunto, che, spesso, i dispositivi usati per rendere la prestazione (si pensi allo *smarthphone*) hanno già inserito di default un *software*, ad esempio, per la geolocalizzazione, senza che sia stato il datore di lavoro a prevederlo.

65 Par. 1.2, cap. 1.

registrati, in quanto è tenuto a rispettare i limiti delineati dal terzo comma, ai fini della tutela della dignità e riservatezza del lavoratore[66].

Per quanto riguarda l'ambito di applicazione del secondo comma e la definizione di strumenti di lavoro, si possono individuare due concetti.

Il primo fa riferimento alla considerazione secondo la quale non esista una definizione ontologica di strumento di lavoro, nel senso che non è possibile catalogare in via astratta gli strumenti riconducibili ad un certo tipo di lavoro.

Quando il lavoratore adempie alla sua obbligazione di lavorare egli è tenuto a rispettare l'oggetto del contratto di lavoro, attraverso il quale il datore di lavoro individua specificamente le mansioni a cui è adibito e, talvolta, è tenuto ad eseguire la prestazione utilizzando gli strumenti indicati e forniti dal datore. Ciò significa che l'individuazione dei possibili strumenti di lavoro non potrà che essere effettuata caso per caso, a seconda delle mansioni specificamente individuate dal potere direttivo dell'imprenditore e dal loro inserimento all'interno dell'organizzazione dell'impresa[67].

In questa prospettiva, il medesimo strumento può assumere la qualità di strumento di controllo o di strumento di lavoro, a seconda di come viene esercitato il potere direttivo, di come conseguentemente deve essere eseguita la prestazione e, infine, delle valutazioni organizzative insindacabili del datore di lavoro.

L'esemplificazione più immediata per illustrare il senso di questo approccio interpretativo è quella riferita agli impianti di geolocalizzazione. Impianti, questi, che sono sempre strumenti di controllo, laddove lascino traccia dei movimenti del lavoratore, ma che possono diventare strumenti di lavoro qualora il dipendente (si pensi al tecnico che effettua interventi sul territorio muovendosi con l'auto aziendale) sia tenuto ad utilizzarli per realizzare la concreta ed effettiva attuazione della prestazione lavorativa, cioè la stessa non possa essere resa senza il ricorrere all'uso di tali strumenti (ad esempio, si fa riferimento al caso il cui il dipendente utilizzi tale sistema per ricevere l'indicazione del luogo ove effettuare l'intervento o per dare conferma dell'avvenuta presa in carico di un servizio o per individuare il percorso più rapido per raggiungere il sito di destinazione e per formalizzare l'avvenuta chiusura dell'operazione). Spetta solo all'imprenditore la valutazione discrezionale sull'opportunità o meno di introdurre tale sistema tecnologico.

---

66 I. ALVINO, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, LLI, vol.2, n. 1, 2016, 23-24.

67 Osserva M. MARAZZA che si preclude all'interprete ogni tentativo di sovrapporre argomentazioni di tipo organizzativo, come possono essere quelle sulla minore o maggiore utilità di quello strumento. In altre parole, non si può autorizzare il giudice a sostituirsi arbitrariamente alle valutazioni tecniche dell'imprenditore per ciò che riguarda l'organizzazione delle mansioni dei suoi dipendenti. In *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore),* WP CSDLE "Massimo D'Antona".IT, 300/2016, 2016, 10.

Recentemente è stata emessa dalla Cassazione la sentenza del 5 ottobre 2016, n. 19922 in tema di monitoraggio dei dipendenti via GPS, la quale ha ritenuto la geolocalizzazione un sistema di controllo generalizzato che non può essere usato per verificare la condotta illecita del dipendente e per legittimarne il licenziamento[68].

In seguito a tale pronuncia sono arrivate da parte dell'Ispettorato Nazionale del Lavoro le istruzioni operative sull'utilizzazione degli impianti di localizzazione satellitare.

Infatti l'Ispettorato ha emanato il 7 novembre 2016 la circolare n. 2/2016 in materia di installazione ed uso di apparecchiature di geolocalizzazione su auto aziendali, chiarendo in che limiti l'installazione di tali sistemi sia soggetta alle garanzie previste dall'art. 4, comma 1.

In particolare, L'Ispettorato ha esplicitato che i sistemi di geolocalizzazione rappresentano, in genere, un elemento "aggiunto" agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa, ma per rispondere ad ulteriori esigenze, ossia quelle di carattere organizzativo, produttivo, per garantire la sicurezza sul lavoro e la tutela del patrimonio aziendale. Ne conseguirebbe che anche i sistemi di controllo via GPS rientrerebbero nel campo di applicazione del primo comma e pertanto le relative apparecchiature potrebbero essere installate solo previo accordo sindacale, ovvero, in assenza, previa autorizzazione da parte dell'Ispettorato Nazionale del Lavoro.

In linea di massima, solo in casi del tutto particolari (come, ad esempio, qualora i sistemi di localizzazione siano installati per consentire il concreto ed effettivo adempimento della prestazione lavorativa, ovvero l'installazione sia richiesta da specifiche normative, come quella che esige l'uso di tali sistemi nel caso di trasporto di portavalori superiore ad un determinato importo) si può ritenere che gli stessi finiscano per essere considerati quali strumenti di lavoro e, in ragione di ciò, si possa prescindere sia dall'intervento della contrattazione collettiva e sia dal provvedimento autorizzativo, ai sensi di quanto previsto dal secondo comma.

Alla luce di tali indicazioni occorre allora ritenere che l'installazione dei sistemi di geolocalizzazione sui veicoli aziendali non necessiti di accordo sindacale o autorizzazione solo in

68 Nel caso concreto la Corte ha escluso che tale controllo possa qualificarsi come difensivo in quanto predisposto *ex ante* a prescindere dal sospetto di un'eventuale violazione da parte del lavoratore, dunque non ne riconosce la legittimità al di fuori dell'ambito di applicazione dell'art. 4. Così facendo, i dati relativi all'attività lavorativa dei dipendenti non potranno essere utilizzati per provare l'inadempimento contrattuale del lavoratore (in senso conforme anche Cass. n. 4375/2010). Viene esclusa così, da tale tipologia di controllo, la finalità di tutela di beni estranei al rapporto di lavoro con riferimento al caso di specie, dal momento che altrimenti "si finirebbe per estendere senza ogni ragionevole limite il concetto di controlli "difensivi" perchè quasi sempre la violazione degli obblighi contrattuali dei dipendenti può generare danni alla società (ed alla sua reputazione) che però costituiscono il "rischio naturale" correlato all'attività imprenditoriale che la legge non consente di limitare attraverso sistemi invasivi della dignità dei lavoratori e comunque senza autorizzazione sindacale".

quei particolari casi in cui siano utilizzati per l'effettivo esercizio della prestazione lavorativa, mentre, in generale, al di fuori di tali ipotesi, richiedono il rispetto delle procedure previste dall'art. 4 comma 1, per cui si dovranno coinvolgere i sindacati o, in mancanza o nel caso di mancato accordo, si dovrà presentare apposita istanza alla DTL (ora all'Ispettorato Nazionale del Lavoro), utilizzando, a tal fine, il *modulo unificato di istanza di autorizzazione all'installazione di impianti di videosorveglianza e all'installazione e utilizzo di impianti e apparecchiature di localizzazione satellitare GPS a bordo di mezzi aziendali*, messo a disposizione dal Ministero del Lavoro. In tale documento si prevedono numerose prescrizioni in materia di installazione ed utilizzo degli strumenti di videosorveglianza e localizzazione. È interessante osservare che in materia di dispositivi di tracciamento dei veicoli, il documento prescriva che gli stessi siano utilizzati al solo fine di rintracciare o monitorare l'ubicazione dei veicoli sui quali sono installati. Quindi, tali dispositivi non saranno utilizzati come strumenti per seguire o monitorare il comportamento o gli spostamenti dei dipendenti. Diverse, invece, sono le prescrizioni in materia di trattamento dei dati ottenuti dagli strumenti, in quanto si prevede che solo i dati pertinenti e non eccedenti potranno costituire oggetto del trattamento (mediante sistemi opportunatamente configurati; art. 3 Codice della privacy). Tali dati si configurano, ad esempio, nella distanza percorsa, nei tempi di percorrenza, nel carburante consumato o nella velocità media del veicolo.

Dunque, è in questa prospettiva che il provvedimento ritiene necessario individuare esattamente quando l'installazione di tali apparecchiature sia strettamente funzionale a rendere la prestazione lavorativa, dedotta in contratto e quando si possa cofigurare quale strumento di controllo preterintenzionale, rispondente alla finalità di soddisfare determinate esigenze tipizzate.

Il secondo concetto riguardante la definizione dello strumento di lavoro è relativo al fatto che il comma secondo faccia esplicitamente riferimento "agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa".

Questo significa che lo strumento di lavoro viene qualificato come quello che il lavoratore impieghi direttamente per lo svolgimento della prestazione, occorrendo in questo modo che egli abbia un ruolo attivo nel suo utilizzo.

Inoltre, ciò implica che lo strumento debba costituire il mezzo funzionale alla corretta esecuzione della mansione oggetto del contratto, ossia della mansione alla quale il datore di lavoro è interessato.

Si deve, dunque, trattare di uno strumento che, sia serva al lavoratore per rendere la prestazione e adempiere all'obbligazione contrattuale e, allo stesso tempo, sia utile al datore di lavoro[69].

69 R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro*, *Riv. it. Dir. Lav.*, n. 1, 2016, 77 ss., per il quale uno strumento di controllo è uno strumento di lavoro se direttamente funzionale allo svolgimento della prestazione lavorativa. M. T. SALIMBENI, *La riforma dell'art. 4 dello Statuto dei lavoratori: l'ambigua risolutezza del*

Senza pretendere che la distinzione tra strumenti di controllo e di lavoro possa risolvere d'incanto tutti i problemi qualificatori che si possono porre nei casi concreti, in conclusione, si può considerare che, per quanto riguarda lo strumento di lavoro, questo è una tipologia particolare di strumento di controllo, che esprime un nesso intrinseco e ineliminabile con l'organizzazione del lavoro. Infatti è lo strumento attraverso il quale è reso possibile l'adempimento della prestazione di lavoro da parte del lavoratore, in osservanza all'obbligo di compiere la propria attività rispettando le disposizioni a lui impartite dall'imprenditore per l'esecuzione e per la disciplina del lavoro (art. 2104 c.c.). Tale nesso funzionale, non presente per lo strumento di controllo che è rispondente ad altre esigenze, può, dunque, giustificare la rimozione dei vincoli rappresentati dalla procedura negoziale o amministrativa richiesta per l'installazione degli impianti dai quali derivi un controllo preterintenzionale, ai sensi dell'art. 4 primo comma.

6.1 Gli strumenti di rilevazione degli accessi e delle presenze.

Il nuovo secondo comma prevede l'esenzione dall'obbligo di autorizzazione, oltre che per gli "strumenti di lavoro", anche per gli "strumenti di registrazione degli accessi e delle presenze". Dunque, il datore di lavoro, anche in questo caso, non sarebbe tenuto né a sottoscrivere accordi con le rappresentanze sindacali, né ad ottenere autorizzazioni da parte dell'Ispettorato Nazionale del Lavoro.

Ciò significa che, anche per questa fattispecie, una volta ottemperati correttamente gli obblighi di informazione al lavoratore (ai sensi del terzo comma), le informazioni acquisite mediante controllo sugli strumenti di registrazione delle presenze e degli accessi sono utilizzabili a tutti i fini connessi al rapporto di lavoro (e quindi anche a quelli disciplinari).

L'esclusione dalla procedura autorizzatoria per tali categorie di strumenti costituisce un'altra delle novità della riforma apportata nel 2015.

Prima della riforma gli strumenti di registrazione dell'inizio e della fine dell'attività lavorativa erano considerati comunque estranei alla fattispecie del divieto assoluto, enunciato nella originaria disciplina del primo comma, in quanto non finalizzati al controllo vessatorio sul lavoratore, essendo il loro scopo quello di registrare i dati temporali necessari per la gestione aziendale e la remunerazione della prestazione (andando ad individuare gli orari di accesso e di uscita e gli straordinari, rilevando la presenza a mensa in correlazione con gli intervalli contrattuali e nel rispetto dei turni aziendalmente stabiliti o la presenza in assemblea al fine del computo delle ore

---

legislatore, Riv. It. Dir. Lav., n. 4, 2015, I, 589 ss., per la quale l'art. 4 co.1 non trova applicazione "soltanto nelle ipotesi in cui il meccanismo che genera il controllo è nella gestione del lavoratore, che lo attiva e lo disattiva per rendere la prestazione".

così impiegate, nel limite delle dieci ore annue durante l'orario di lavoro secondo quanto stabilito dall'art. 20 St. lav.)[70]. Questione questa che, in passato, non aveva mancato di creare un dibattito giurisprudenziale, che vedeva contrapporsi l'orientamento per il quale l'utilizzo del *badge* per l'accesso e l'uscita dal luogo di lavoro fosse da qualificarsi come strumento di controllo a distanza, con conseguente applicazione dell'art. 4[71] e l'orientamento opposto, secondo cui il controllo in ingresso e in uscita non è qualificabile come controllo a distanza, individuando, opportunamente, la sua motivazione nel considerare tale tipo di controllo non riguardante l'attività lavorativa, nell'ottica di un bilanciamento più ragionevole degli interessi contrapposti[72].

L'interpretazione che si deve dare al dettato normativo vigente è, in realtà, nel senso di comprendere nella categoria degli strumenti di rilevazione degli accessi e delle presenze (i quali, alla luce della nuova norma si ricorda, potranno essere installati senza la preventiva autorizzazione) non solo quelli che registrano l'inizio e la fine della giornata lavorativa, ma anche quelli che registrano eventuali spostamenti del lavoratore effettuati all'interno dell'orario e dell'ambiente di lavoro, come possono essere, ad esempio, gli strumenti di rilevazione degli accessi a specifici locali aziendali ovvero strumenti deputati a registrare il passaggio da un ufficio o reparto ad un altro, con il fine, quindi, di individuare il personale presente in una determinata area in un certo momento[73].

Volendo individuare nello specifico delle ipotesi esemplificative, per quanto riguarda gli strumenti di registrazione delle presenze e degli accessi (in locali aziendali ad accesso riservato, come i centri di ricerca, progettazione, sperimentazione) si possono annoverare i *badge* (tessere elettroniche), i sistemi di rilevazione antropobiomentrici, che rilevano l'identità del lavoratore tramite corrispondenza delle impronte digitali o palmari o dell'iride con dati personali già memorizzati[74] e persino microchip sottocutanei.

---

70 A. DEL NINNO, *In vigore la riforma dell'art. 4 dello Statuto dei Lavoratori sui controlli a distanza: il decreto legislativo 14 Settembre 2015 n. 151, privacy dei lavoratori e nuove regole*, *Diritto e Giustizia*, 2015, 9.

71 Cass., sez. lav., sentenza del 17 luglio 2007, n. 15892 include tali strumenti fra quelli richiedenti l'accordo sindacale o l'autorizzazione amministrativa, osservando che "il controllo a distanza sull'orario 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 dall'art. 4, comma 2".

72 Già in Trib. Milano 26 marzo 1994, in Orient. Giur. Lav., 1994, 23.

73 Diversamente, M. T. SALIMBENI, interpretando restrittivamente, ritiene che il legislatore faccia esclusivamente riferimento ai sistemi di controllo di ingresso e di uscita dall'azienda necessari ad appurare il rispetto dell'orario di lavoro. Tale interpretazione annullerebbe, peraltro, la portata innovativa della riforma in quest'ambito. Così in *La riforma dell'art. 4 dello Statuto dei Lavoratori: l'ambigua risolutezza del legislatore*, *Riv. it. Dir. Lav.*, n. 4, 2015, I, 589ss.

74 In questa casistica si pensi anche agli accessi digitali alle reti informatiche, resi possibili anche grazie all'utilizzo di dati biomentrici. Il Garante della privacy è intervenuto, a questo proposito, con il provvedimento generale in tema di biometria del 12 novembre 2014, n. 513 (doc. web. n. 3556992), con il quale ha adottato le Linee guida relative al

Quest'ultima ipotesi fa riferimento ad un esperimento condotto da un'azienda svedese, che opera nel campo dell'hi-tech (l'Epicenter), avviato al fine di combattere l'assenteismo sul posto di lavoro e la scarsa produttività. Alcuni lavoratori dell'azienda sono stati disposti a farsi iniettare un chip sottocutaneo, che può essere utilizzato per aprire porte, sbloccare dispositivi o pagare i distributori automatici[75]. In questo modo, il chip non solo punta a migliorare la vita aziendale, ma permette, potenzialmente, di tracciare con precisione i movimenti del dipendente all'interno dell'azienda.

In ogni caso, qualunque sia la modalità attraverso la quale si attua la rilevazione degli accessi e delle presenze e nonostante gli strumenti a tal fine impiegati non richiedano l'accordo o l'autorizzazione, si ricorda che il datore di lavoro non ha libertà assoluta circa la loro installazione, la quale dovrà essere rispettosa delle regole poste dal Codice della privacy e dal Garante.

In questa sede è opportuno segnalare la recente pronuncia della Corte di Cassazione[76], che ha confermato l'illegittimità del licenziamento di un lavoratore, rigettando il ricorso dell'azienda, poiché ha ritenuto che il recesso del rapporto non potesse basarsi sui dati forniti dal *badge* aziendale in uso ai dipendenti, il quale forniva informazioni non solo sull'orario di ingresso e di uscita, ma anche le sospensioni, i permessi e le pause. La decisione della Corte si è basata sulla considerazione che il *badge*, anziché fungere da mero rilevatore di presenza, funzionasse piuttosto come strumento dal quale potesse derivare un controllo a distanza del lavoratore ed, in quanto tale, a norma dell'art. 4 comma 1 Stat. Lav., presupporrebbe, per il suo impiego, il previo accordo con le rappresentanze sindacali, o in mancanza, l'autorizzazione dell'Ispettorato del lavoro. In altri termini, si è voluto affermare che, qualora lo strumento, predisposto dal datore di lavoro, di rilevazione dei dati di entrata e di uscita dall'azienda permetta anche il controllo dell'osservanza dei doveri di diligenza nel rispetto dell'orario di lavoro e della correttezza nello svolgimento della prestazione, questo vada, in realtà, a configurare uno strumento di controllo a distanza avente ad oggetto il giusto adempimento dell'attività lavorativa, per il quale è necessaria, per la sua legittimità, la previa procedura di cui al primo comma. Inoltre, è stato ribadito che neppure l'esigenza di evitare condotte illecite da parte dei dipendenti, quando questi comportamenti riguardino l'esatto adempimento della prestazione, possa giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore. Piuttosto, il controllo datoriale può essere giustificato nel caso in cui l'oggetto sia l'accertamento di condotte illecite e lesive del patrimonio aziendale nonché

---

riconoscimento biometrico e firma grafometrica che delimitano i dati biometrici utilizzabili (voce, impronte digitali) e fissano regole di trattamento per l'accesso a sistemi informatici e ad aree riservate.

75 https://www.tomshw.it/chip-sottopelle-lavoro-comodita-preoccupa-84656

76 Cass., sez. lav., 13 maggio 2016, n. 9904.

dell'immagine aziendale, laddove quindi si vogliano tutelare beni estranei al rapporto di lavoro, poiché, in questo caso, si sarebbe al di fuori del campo di applicazione della norma statutaria[77].
Alla luce di questa sentenza si rileva la corretta volontà giurisprudenziale di ricondurre in un'ottica di opportuno bilanciamento quelle che sono le contrapposte esigenze delle parti contrattuali, imprimendo una direzione al percorso interpretativo della norma nel senso di una presa d'atto delle nuove condizioni di lavoro dettate dall'avvento della tecnologia e dal suo preponderante ed inevitabile impiego al servizio dell'attività lavorativa, sia per il vantaggio datoriale quanto del dipendente, e delle nuove possibilità di controllo da ciò occasionate e nel senso di una elaborazione degli orientamenti interpretativi passati e della delineazione di un'interpretazione evolutiva, che guarda al futuro quale nuovo modello di riferimento[78].

7. Il nuovo comma 3 dell'art. 4 Stat. Lav. L'intreccio tra lo Statuto dei lavoratori e la disciplina della *privacy.*

L'impiego e l'installazione di strumenti dai quali derivi un controllo preterintenzionale dell'attività lavorativa, così come l'uso degli strumenti adottati dal lavoratore nello svolgimento della stessa e degli strumenti di registrazione degli accessi e delle presenze pone il problema della legittimità dell'utilizzo, da parte del datore di lavoro, di tutte quelle informazioni raccolte per il loro tramite.
Tali strumenti, in un contesto in cui lo sviluppo tecnologico è continuo ed esponenziale, consentono un controllo che può diventare invasivo della sfera privata del lavoratore, ad esempio, attraverso il monitoraggio della casella di posta elettronica o la verifica degli accessi ad Internet o l'elencazione dei siti visitati durante l'orario di lavoro o nelle pause. Da qui, sorge la necessità di coordinare la disciplina dettata dal nuovo art. 4 dello Statuto dei lavoratori con quella della *privacy*.
A tal proposito, fondamentale appare il comma 3 dell'articolo anzidetto (che, si ricorda, viene inserito dal Legislatore all'interno del Titolo I dello Statuto, intitolato "Della libertà e dignità del lavoratore")[79].
Come emerge dal testo della norma, diverse sono le condizioni poste alla legittima utilizzabilità (a tutti i fini connessi al rapporto di lavoro e dunque anche a quello disciplinare) delle informazioni raccolte mediante dispositivi audiovisivi o di controllo a distanza.

77 Par. 4., cap. 1.

78 A. TEA, *Controlli a distanza: spunti problematici e sviluppi interpretativi*, *il Lav. nella giur.*, 1/2017, 24.

79 Art. 4, comma 3, Stat. Lav.:"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".

Un limite generale deriva, anzitutto, dall'osservanza delle disposizioni di cui ai commi 1 e 2 dell'articolo in esame, che, si ricorda, disciplinano le finalità di impiego e le modalità di installazione degli strumenti di rilevazione a distanza, degli strumenti di lavoro e degli strumenti di registrazione degli accessi e delle presenze. Dal mancato rispetto di tali previsioni, infatti, possono conseguire importanti limitazioni circa la fruibilità dei dati illegittimamente raccolti[80].

La seconda parte della disposizione introduce poi due ulteriori limiti, nuovi, che in nulla rimandano ai commi precedenti: al lavoratore deve essere data adeguata informazione circa le modalità d'uso degli strumenti di rilevazione e le modalità di effettuazione dei controlli e, nel contempo, deve essere rispettata la disciplina del Codice della privacy.

In tale contesto, appare opportuna una prima considerazione. Mentre i commi 1 e 2 dell'art. 4 Stat. Lav. dettano disposizioni sull'opportunità circa l'impiego e l'installazione degli strumenti e sul conseguente reperimento di dati attraverso tali apparecchiature di controllo, il comma 3 introduce limiti e restrizioni che attengono invece alla possibilità, per colui che pone in essere il controllo, il datore di lavoro, di utilizzare le informazioni raccolte.

Lo scenario che si viene ad analizzare è sempre quello che deriva dalla necessità di bilanciare due opposte esigenze, consistenti, da un lato, nel legittimo esercizio, da parte del datore di lavoro, del suo potere di controllo, e, dall'altro, nella necessità, per il lavoratore, di vedere garantiti e tutelati i suoi diritti di libertà e di riservatezza.

Ecco allora evidente l'opportunità di confrontare e, soprattutto, coordinare, due differenti modelli normativi, quali lo Statuto dei lavoratori, espressione specifica della volontà di tutelare il lavoratore quale parte debole del rapporto di lavoro ed il Codice della privacy, ovvero il d.lgs. n. 196/2003 destinato, come si vedrà di seguito, ad essere, per il momento, affiancato dal recente Regolamento UE 2016/679[81].

---

80 La conseguenza della mancata osservanza dei commi 1 e 2 si ritiene essere l'inutilizzabilità dei dati illegittimamente raccolti, e non solo laddove manchi l'adeguata informazione o il rispetto della disciplina della *privacy*, condizioni richieste dalla parte seguente del testo del comma terzo, ma anche laddove l'utilizzo di tali dati non sia compatibile con gli scopi individuati dal trattamento (come anche affermato dal principio di finalità di cui all'art. 11 co.1, lett. b del Codice della privacy). In altri termini, si fa riferimento alle esigenze organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale, che configurano appunto la specifica finalità per la quale il controllo verrebbe posto in essere. Qualora mancasse la finalità sarebbe da escludere l'utilizzabilità dei dati raccolti ai fini connessi al rapporto di lavoro. Cfr. A SITZIA, *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali*, Cedam, Padova, 2013, 43 ss.; E. DAGNINO, *Tecnologie e controlli a distanza*, *Dir. Rel. Indu*., n. 4, 2015, 988 ss.

81 Il Regolamento Ue, n. 2016/679, intitolato "Regolamento Generale sulla Protezione dei Dati", diverrà applicabile in via diretta in tutti gli Stati Membri a partire dal 25 maggio 2018. Gli Stati membri hanno, dunque, nel frattempo, la facoltà di armonizzare ed integrare la disciplina interna con quella prevista dal Regolamento, il quale a partire dalla suddetta data sarà comunque direttamente applicabile, andando a sostituire la difforme disciplina interna in materia di trattamento dei dati personali.

Dal necessario raccordo tra le due discipline emerge un primo problema applicativo, ovvero se il rinvio alla disciplina della *privacy* contenuto nell'articolo 4 debba ritenersi limitato all'impianto normativo del Codice o, al contrario, esteso a fonti ad esso esterne. Il riferimento è alle Linee guida emanate dall'Autorità Garante ex art. 154, comma 1, lettera c)[82] del d.lgs. 196/2003 in materia di trattamento dei dati personali dei lavoratori, recuperati mediante l'impiego di strumenti specifici. Pacifica, proprio in virtù del suddetto articolo, si ritiene la posizione secondo cui il rinvio generico al Codice della privacy deve includere altresì le norme ed i provvedimenti secondari, regole esecutive dei principi più generali espressi dal Codice. Nei paragrafi a seguire, dunque, verranno esplicate tanto le norme di principio e i criteri in base ai quali deve essere vagliata la legittimità del controllo datoriale e dell'uso delle informazioni raccolte, quanto il provvedimento generale del 1 Marzo 2007 del Garante della privacy recante le Linee guida per posta elettronica e Internet.

A tal proposito è da rilevare che, proprio in ragione del fatto per cui la disciplina della *privacy* si compone anche di tutti i provvedimenti secondari emanati dal Garante, il datore di lavoro si troverà a dover rispettare tutta una serie di accorgimenti preventivi, ispirati alle finalità espresse all'art. 2 del Codice della privacy[83], i quali dovranno essere da lui applicati prima ancora della delineazione ed emanazione di una policy aziendale o del rilascio delle informazioni necessarie al lavoratore per essere adeguatamente informato.

Il secondo interrogativo che ci si pone è quello relativo ai rapporti tra le due normative in termini di eventuale prevalenza dell'una sull'altra, in considerazione del modo in cui l'ordinamento regola le relazioni tra noma speciale e norma generale.

Le discipline devono, secondo la nuova formulazione del terzo comma, concorrere ed integrarsi tra loro[84], e, a seconda delle varie interpretazioni dottrinali, in tale confronto tra le due fonti normative andrebbe a prevalere il riferimento alla disciplina della *privacy* laddove si consideri generalmente applicabile (anche in relazione alla normativa giuslavoristica) la previsione di inutilizzabilità dei

82 Articolo secondo il quale il Garante può prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti.

83 Art. 2, comma 1: "Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".

84 La novità apportata dal comma 3 risiede proprio in questa compenetrazione tra la disciplina giuslavoristica e la disciplina sulla tutela della *privacy*. In questo senso si ritiene che tale collegamento abbia introdotto tutele rafforzate e nuovi limiti al potere di controllo datoriale. Così per M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona – 300/2016, 24; A. DEL NINNO, *In vigore la riforma dell'art. 4 dello Statuto dei lavoratori sui controlli a distanza: il decreto legislativo 14 settembre 2015 n. 151, privacy dei lavoratori e nuove regole*, *Diritto e Giustizia*, 2015, 13; R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015)*, *Riv. ita. Dir. Lav.*, n. 1, 2016, 77 ss.

dati trattati in violazione della disciplina in materia di trattamento dei dati personali come stabilito dall'art. 11 comma 2 del Codice[85], oppure andrebbe a prevalere in ogni caso quanto stabilito dall'art. 4 Stat. Lav., in ragione della sua natura di norma speciale che disciplina la tutela della riservatezza di un soggetto interessato qualificato (cioè il lavoratore) rispetto ad uno strumento di trattamento del dato tipizzato (qual è lo strumento di controllo a distanza)[86]. Dunque, secondo quest'ultimo indirizzo, il d.lgs. 196/2003 deve ritenersi applicabile nella misura in cui non venga derogato espressamente dall'art. 4 dello Statuto[87].

È interessante notare come, in dottrina, buona parte degli interpreti si sia espressa, in merito al terzo comma dell'art. 4, unicamente nella prospettiva in cui l'utilizzo delle informazioni raccolte venga effettuato a fini disciplinari o sanzonatori, tralasciando l'eventualità secondo la quale le informazioni ricavate possano essere, al contrario, utilizzate a fini premiali[88]. Questo porterebbe entrambe le parti a far valere i propri interessi nel rapporto di lavoro, per il lavoratore l'interesse a vedersi riconosciuta la maggiore qualità del lavoro svolto o di contrattare migliori condizioni economiche e normative del suo impiego e per il datore di lavoro l'interesse all'aumento della produttività incentivato mediante la premiazione dell'alta qualità della prestazione ricevuta. Secondo questa visione, si potrebbe ipotizzare un cambiamento del rapporto tra i sindacati delle parti, che vedrebbe basarsi l'obiettivo del raggiungimento di un accordo non solo in vista della previsione di sanzioni, ma anche della previsione di premi.

---

85 E. DAGNINO, *Tecnologie e controlli a distanza*, *Dir. Rel. Indu*., n. 4, 2015, 988-989.

86 M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona – 300/2016, 26.

87 "La questione è di grande importanza perché sta a significare che l'esplicita autorizzazione legislativa al trattamento dei dati per tutti i fini connessi al rapporto di lavoro (comma 3), previo il rispetto dei commi 1 e 2 e fermo l'adempimento dell'obbligo di informativa, supera ogni diversa previsione del Codice Privacy in materia di consenso al trattamento e/o di finalità dello stesso". M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona – 300/2016, 26. Così anche per M. T. SALIMBENI, che ritiene necessario un prevenivo confronto con il rispetto della normativa prevista dall'art. 4. In *La riforma dell'art. 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, *Riv. Ita. Dir. Lav*., n. 4, 2015, I, 589 ss.

88 Un'opinione in tal senso è stata ipotizzata da M. MARAZZA, per il quale l'utilizzo dei dati per finalità (legittime) diverse da quelle connesse, in senso stretto, al rapporto di lavoro configurerebbe una prospettiva non trascurabile, poiché non vi è dubbio che gli strumenti di controllo a distanza più tecnologicamente avanzati consentono di tracciare e di documentare lo spessore professionale di una prestazione di lavoro anche in termini di rendimento medio. E quindi, pur tenendo conto dei limiti al trattamento dei dati derivanti dalla c.d. "profilazione", questi fornirebbero elementi di valutazione che, con il consenso della persona, potrebbero assumere rilevanza anche ai fini occupazionali. Inoltre non sarebbe da escludere che possa essere lo stesso lavoratore a voler direttamente utilizzare i dati raccolti dal datore, ad esempio, per negoziare le condizioni economiche e normative del suo impiego. *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona – 300/2016, 8-9.

Infine, l'intreccio tra le due fonti normative si completa con la modifica, apportata dall'art. 23 del d.lgs. 151/2015, all'art. 171[89] del d.lgs. 196/2003.

Rispetto alla formulazione precedente la riforma[90], il Legislatore ha previsto la sostituzione del riferimento relativo alla violazione dell'art. 114 del Codice con quello relativo alla violazione dell'art. 4, commi 1 e 2, Stat. Lav., con ciò configurando una sanzione, in virtù del richiamo diretto alla norma statutaria, di natura lavoristica[91] e non più di natura relativa alla disciplina della *privacy*[92].

Ciò premesso, si vanno ora ad esaminare, nel dettaglio, le condizioni di utilizzabilità dei dati di cui si è fatto prima cenno.

8. Le condizioni di utilizzabilità dei dati. L'adeguata informazione.

La prima condizione posta dall'art. 4, comma 3, dello Statuto all'utilizzabilità dei dati raccolti mediante strumenti di rilevazione a distanza consiste nella necessità che il lavoratore sia stato informato tanto delle modalità d'uso degli strumenti stessi quanto delle modalità di effettuazione dei controlli.

Dovute sono delle brevi precisazioni preliminari.

Anzitutto, la norma nulla dice circa le modalità mediante le quali l'informazione deve essere resa, ovvero la forma che la stessa deve assumere (e così neanche l'art. 13 del Codice della privacy

89 Art. 171, d.lgs. 196/2003: "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".

90 Vecchia formulazione per la quale in ipotesi di violazione dell'art. 114 ("Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300") si sarebbero applicate le sanzioni di cui all'art. 38 Stat. Lav.

91 La sanzione assume una natura "lavoristica" proprio in quanto l'art. 171 del Codice della privacy ora colpisce ogni violazione diretta dell'art. 4 Stat. Lav., al di là di qualunque aspetto sul trattamento dei dati personali. Si pensi all'esempio per il quale sia sanzionabile il mancato rispetto della procedura di cui al comma 1 dell'art. 4, a prescindere e anche prima del trattamento dei dati personali conseguente all'impiego ed all'installazione degli strumenti.

92 Secondo A. DEL NINNO l'aver previsto, per la prima volta, una sanzione diretta per la violazione dell'art. 4 Stat. Lav. (norma "lavoristica") in un testo normativo diverso (il Codice della privacy) configura un rilievo singolare, dal quale l'Autore deduce una visione sistematica ed un timore quasi reverenziale da parte del Legislatore nei confronti di un'eventuale (e non intervenuta in questa parte) modifica dello Statuto. Inoltre considera che una modifica, che sarebbe stato opportuno inserire proprio nell'art. 38 Stat. Lav., aggiungendo le ipotesi di violazione dell'art. 4, sia stata invece inserita in una norma, l'art. 171, dedicata alle sanzioni penali previste per la violazione del trattamento dei dati personali, che ora risulta applicabile anche a casi che nulla hanno a che fare con il trattamento dei dati. *In vigore la riforma dell'art. 4 dello Statuto dei lavoratori sui controlli a distanza: il decreto legislativo 14 settembre 2015 n. 151, privacy dei lavoratori e nuove regole, Diritto e Giustizia,* 2015, 14. Anche E. DAGNINO sottolinea la singolarità della modifica apportata secondo una tecnica normativa per la quale l'applicazione della sanzione prevista dallo Statuto venga affidata ad una fonte esterna. In *Tecnologie e controlli a distanza, Dir. Rel. Indu.*, n. 4, 2015, 988-989.

relativo all'informativa sul trattamento dei dati personali). Potrebbe, dunque, ritenersi ammissibile la comunicazione orale, sebbene essa non si ritenga opportuna in considerazione soprattutto della necessità che la stessa possa essere prodotta in giudizio nell'ambito dell'eventuale controversia col lavoratore. Viene così suggerita la forma scritta al titolare che voglia precostituirsi una prova comoda che dimostri il suo adempimento all'obbligo di informativa[93]. Occorre poi rilevare che la norma precisa che l'informazione debba essere "adeguata", quindi completa e chiara, al fine di permettere al soggetto debole di comprendere quanto la stessa dispone e si può dubitare del fatto che la forma orale possa soddisfare a pieno tale esigenza di tutela.

Per quanto riguarda la questione della conoscenza dell'adeguata informazione, un'opinione dottrinale ritiene sia necessario che il lavoratore dia conferma individuale dell'avvenuta ricezione dell'informativa[94], mentre quella opposta ritiene sia sufficiente anche una comunicazione generalizzata[95]. In questo caso sarebbe opportuno che il lavoratore venga quantomeno avvisato del rilascio dell'informativa e che la documentazione relativa (digitale o cartacea) sia accessibile, eventualità questa collegabile alla previsione secondo cui il dipendente sarebbe tenuto ad aggiornarsi sui regolamenti interni dell'azienda e sulla loro modificazione, dovendo egli osservarli nello svolgimento della sua prestazione (artt. 2094 e 2104 c.c.).

Per ciò che concerne l'elemento oggettivo dell'adeguata informazione, è da ritenersi, innanzitutto, che questa debba riferirsi, siano essi strumenti di controllo o strumenti di lavoro, anche alle

93 Sarebbe difficile dimostrare, in un eventuale giudizio instaurato a seguito di licenziamento disciplinare comminato per il mancato rispetto delle regole individuate nell'informativa, che il lavoratore abbia in realtà ricevuto le prescrizioni relative, essendo la comunicazione orale inadatta a formare la prova. "Ne consegue che in un eventuale procedimento disciplinare il dipendente, pur in presenza del rispetto dell'art. 4, potrà eccepire la violazione della normativa *privacy* come causa di inammissibilità delle prove eventualmente raccolte dal datore di lavoro". Dunque, il rispetto delle prescrizioni ex art. 4 non tutela il datore di lavoro nel caso in cui esso non abbia rispettato anche le prescrizioni inerenti alla disciplina della *privacy*. E. OLIMPIA POLICELLA, *Controlli dei dipendenti: gli impianti audiovisivi nel nuovo art. 4 dello Statuto dei lavoratori*, *Diritto24*, 2015, su http://www.diritto24.ilsole24ore.com/art/dirittoLavoro/2015-09-15/controlli-dipendenti-impianti-audiovisivi-nuovo-art-4-statuto-lavoratori--161229.php?preview=true .

94 A. MARESCA, *Jobs Act, come conciliare il potere di controllo e tutela della dignità e riservatezza del lavoratore*, in *Forum Tuttolavoro*, 2016. In questo senso si nota che nella circolare diffusa da Confindustria dopo l'entrata in vigore del nuovo art. 4 sia stata individuata l'eventualità di fornire l'adeguata informazione sia al singolo lavoratore, sia a gruppi di lavoratori aventi le stesse mansioni e sia a gruppi di lavoratori aventi mansioni differenti ma adoperanti gli stessi strumenti, purché la modalità scelta, qualunque essa sia, garantisca la comunicazione personale.

95 R. DEL PUNTA considera sufficiente il semplice promovimento del regolamento *privacy* aziendale, in *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D.lgs. n. 151/2015)*, *Riv. ita. dir. Lav.*, n. 1, 2016, 81; M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona". IT – 300/2016, 31.

apparecchiature installate prima della riforma, non operando la norma alcuna distinzione in argomento.

Dal punto di vista contenutistico, l'adeguata informazione, di cui al terzo comma, deve essere relativa alle modalità d'uso degli strumenti (indifferentemente rientranti nei commi 1 o 2) e alle modalità di effettuazione dei controlli.

Entrambi gli adempimenti hanno una caratterizzazione diversa da quella che connota l'informativa prevista dall'art. 13 del Codice della privacy[96], in quanto devono presentare un contenuto più specifico, il quale si riferisce in modo mirato all'utilizzo degli strumenti di controllo impiegati in azienda ed alle prassi con cui si effettua il controllo medesimo, che è espressione tipica del potere direttivo del datore di lavoro. Si nota una sovrapposizione tra l'art. 13 e la previsione di cui all'art. 4 (il quale è, comunque, una disposizione che impone la comunicazione all'interessato dell'esistenza dei controlli e delle "modalità di trattamento cui sono destinati i dati", prescrizione quest'ultima indicata dall'art.13) almeno per ciò che concerne la messa a conoscenza delle modalità di effettuazione dei controlli, poiché si considera che questa sia pur sempre una modalità, anche se qualificata, di trattamento dei dati. Ad ogni modo, il contenuto dell'informativa di cui all'art. 4 presenta delle peculiarità che ne giustificano, anche da un punto di vista formale, un'autonoma valorizzazione. Da ciò deriva l'opportunità di contenere l'adeguata informazione e le modalità in cui si estrica in appositi documenti aziendali separati rispetto alla documentazione relativa alle regole sulla disciplina della *privacy*[97].

In particolare, la comunicazione delle modalità d'uso degli strumenti, mostrando una connotazione più giuslavoristica perché riconducibile ad una manifestazione del potere direttivo datoriale, si ritiene possa essere contenuta in *policy* aziendali, che regolamentano tali modalità a partire da categorie omogenee di strumenti. In questo caso, tuttavia, il contenuto dell'informativa deve essere differenziato a seconda che l'uso sia da riferire a strumenti di controllo o di lavoro, in quanto, per i primi l'informativa sarà inerente alla descrizione dell'utilizzo che il datore di lavoro si riserva di

96 Principalmente, l'art. 13 prevede che l'interessato o la persona presso la quale sono raccolti i dati personali siano previamente informati oralmente o per iscritto circa: a) le finalità e le modalità del trattamento cui sono destinati i dati; b) la natura obbligatoria o facoltativa del conferimento dei dati; c) le conseguenze di un eventuale rifiuto di rispondere; d) i soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei medesimi; f) gli estremi identificativi del titolare.

97 Già nelle Linee guida per la posta elettronica ed Internet del 2007 il Garante aveva prescritto ai datori di lavoro (in aderenza con quanto prescritto dall'art. 154 co.1, lett. c), di "indicare, chiaramente ed in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli" e ciò mediante l'adozione di un disciplinare interno, redatto in modo chiaro e senza formulazioni generiche, da rendere noto ai lavoratori. Punti 3.1 e 3.2.

fare, mentre per gli strumenti di lavoro l'informativa si occuperà delle prescrizioni che il lavoratore è tenuto a seguire nello svolgimento della sua prestazione.
La comunicazione delle modalità di effettuazione dei controlli si ritiene si compia, come già accennato, attraverso documenti separati, comunque destinati ad integrarsi vicendevolmente, e ciò partendo dalla considerazione secondo cui l'informativa, resa ai sensi dell'art. 13, assuma una veste più generale (esplicitando infatti i principi del trattamento dei dati), la quale poi viene integrata, nelle *policy* aziendali, da più specifiche indicazioni richieste dalla particolarità insita in ogni categoria di strumenti dai quali derivi un controllo.

8.1 Le condizioni di utilizzabilità dei dati. Il rispetto del Codice della privacy.

Occorre preliminarmente ribadire che il richiamo operato dall'art. 4, comma 3, dello Statuto dei lavoratori deve necessariamente ritenersi non già limitato all'impianto normativo del Codice della privacy, bensì debba essere esteso ai provvedimenti esecutivi, emanati dal Garante nell'esercizio dei suoi poteri.
Per quanto in questa sede rileva, verranno illustrati anzitutto i principi generali che governano la disciplina del trattamento dei dati, rimandando l'analisi delle Linee guida, già menzionate,, al paragrafo successivo, in quanto di contenuto specifico e meritevole di separata trattazione.
Il datore di lavoro è tenuto a rispettare, oltre che la prescrizione circa l'adeguata informazione, i determinati principi esplicati nel Codice della privacy (insieme agli atti specifici emanati dal Garante), al fine della raccolta legittima dei dati dei dipendenti ottenuti ed al loro utilizzo legittimo e ciò in virtù dello specifico rinvio operato dall'art. 4 Stat. Lav. al d.lgs. 196/2003. È opportuno rilevare che soltanto con la normativa sulla *privacy* l'ordinamento si sia spinto a regolare i singoli atti nei quali si estrinseca il potere datoriale di controllo a distanza, attraverso la previsione di limiti al suo esercizio, che si traducono in corrispondenti diritti soggettivi del lavoratore interessato[98].
Dalla lettera dell'art. 3 del Codice[99], che introduce il principio di necessità nel trattamento dei dati, si evince che l'utilizzazione dei dati personali da parte del datore di lavoro è ammessa esclusivamente qualora la finalità perseguita non possa essere soddisfatta altrimenti, ad esempio attraverso il trattamento di dati anonimi, che precludono l'immediata identificazione del singolo

98 R. DEL PUNTA attribuisce all'avvento del Codice della privacy e della sua disciplina non solo la consapevolezza della possibilità di messa in atto del controllo, ma anche consapevolezza dei confini entro i quali può essere esercitato. *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. lgs. N. 151/2015), Riv. ita. dir. lav*., n. 1, 2016, 83 ss.
99 Art. 3, Principio di necessità nel trattamento dei dati: "I sistemi informativi e i programmi informatici devono essere 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 possano essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".

lavoratore. Infatti, i dati ottenuti, attraverso gli strumenti dai quali sia derivato un controllo, non possono essere impiegati se gli stessi potevano essere raccolti in forma anonima, come avviene mediante l'utilizzo di "dati aggregati", cioè dati che possono essere raccolti e trattati con riferimento ad un gruppo di lavoratori della stessa area o che fanno uso degli stessi strumenti di lavoro, i quali non permettono la conoscenza dell'identità del singolo dipendente risalendo dall'attività da lui svolta. A tal proposito, al datore di lavoro sarà concesso di "disaggregare" i dati relativi a gruppi di lavoratori, procedendo quindi ad un controllo mirato, ma solo a fronte, da un lato, della configurazione di *policy* aziendali ispirate alla regola della gradualità dei controlli, e, dall'altro, della sussistenza di elementi che facciano rinvenire la necessità di un tale trattamento dei dati individuali, come ad esempio laddove si sia in presenza di una presunta violazione degli obblighi contrattuali da parte del dipendente, oppure, in generale, laddove un tale trattamento sia richiesto in virtù della verifica circa la finalità perseguita nel singolo caso, connessa alla gestione del rapporto di lavoro[100].

Altri principi, diversi ma tra loro connessi, sono enunciati dall'art. 11.

Anzitutto, il principio di correttezza (art. 11, comma 1, lett. a)[101], secondo il quale il trattamento dei dati personali deve avvenire nel rispetto dei fondamentali parametri di lealtà e buona fede.

Tale esigenza emerge in maniera ancora più evidente nell'ambito del rapporto di lavoro, caratterizzato da uno squilibrio fisiologico delle parti contrattuali che impone la tutela qualificata del soggetto debole (il lavoratore), il quale deve essere informato previamente ed in maniera chiara delle caratteristiche dei trattamenti di dati raccolti mediante l'impiego di strumenti attribuitigli per lo svolgimento della prestazione lavorativa.

Il principio di correttezza viene, dunque, ad intersecarsi ed a confondersi con il principio di trasparenza, il quale ultimo pervade tutto l'apparato normativo regolatore della *privacy*. È stato sottolineato come tale concetto di trasparenza, in ambito lavorativo, non debba essere inteso come conoscenza del singolo atto di controllo, bensì come consapevolezza, acquisita mediante l'informazione, di poter essere controllato e delle modalità attraverso le quali il controllo può essere operato [102]. Il rispetto del principio di trasparenza implica, oltretutto, per il datore di lavoro, l'onere di indicare, chiaramente ed in modo particolareggiato, quali siano le modalità di utilizzo ritenute

100 M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona". IT – 300/2016, 29.

101 "I dati personali oggetto di trattamento sono trattati in modo lecito e secondo correttezza".

102 R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. lgs. N. 151/2015)*, *Riv. ita. dir. lav.*, n. 1, 2016, 83 ss.

corrette degli strumenti affidati al lavoratore e se, in che misura o con quali modalità verranno effettuati i controlli[103].

Alla lettera b) della medesima norma, il Legislatore impone che i dati oggetto del trattamento vengano raccolti e registrati solo per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi.

Viene così enunciato il principio di finalità, in virtù del quale il trattamento può considerarsi lecito soltanto nella misura in cui sussista alla sua base una ragione che lo giustifica, che deve essere, oltre che legittima, dichiarata in maniera esplicita[104].

In materia giuslavoristica, è lo stesso art. 4 dello Statuto ad esplicitare il fine legittimo. Infatti, da un lato, il controllo deve essere finalizzato a garantire la sicurezza, la continuità aziendale e quindi a prevenire e reprimere inadempimenti ed illeciti, dall'altro, le informazioni raccolte nel rispetto di quanto imposto dalla norma e, nel contempo, dalla normativa sulla *privacy* sono utilizzabili a tutti i fini connessi al rapporto di lavoro. Ciò configura un'estensione delle possibilità di utilizzo dei dati raccolti indubbiamente notevole, ma non certo illimitata, tant'è che la legittimità e determinatezza del fine perseguito attraverso il trattamento (nonché della proporzionalità, correttezza e non eccedenza di quest'ultimo) escludono l'ammissibilità di controlli massivi ed, insieme, impongono una gradualità nella diffusione e nella tipologia del monitoraggio tale da rendere residuali i controlli troppo invasivi, i quali vengono legittimati solo a fronte della individuazione di situazioni anomale[105].

I dati personali raccolti nonché le modalità del loro trattamento devono poi essere pertinenti e non eccedenti rispetto alle finalità perseguite. In questo modo i principi di pertinenza e non eccedenza si riassumono nel principio di proporzionalità, espresso dalla lettera d) dell'art.11, il quale impone che i dati raccolti siano pertinenti al fine esplicitato e trattati nella misura meno invasiva possibile della sfera del singolo[106].

---

103 A. DEL NINNO fa anche riferimento alla disciplina di settore di cui al d.lgs. 81/2008 sulla sicurezza sui luoghi di lavoro in materia di "uso di attrezzature munite di videoterminali", ove si esclude la possibilità del controllo informatico all'insaputa dei lavoratori. *In vigore la riforma dell'art. 4 dello Statuto dei lavoratori sui controlli a distanza: il decreto legislativo 14 settembre 2015 n. 151, privacy dei lavoratori e nuove regole*, *Diritto e Giustizia*, 2015, 12.

104 Inoltre si può arrivare a ritenere che il principio di finalità sia in sostanza un principio di trasparenza, poiché, per effettuare un trattamento dei dati, occorre che esso sia stato dichiarato esplicitamente e che ne siano definite le finalità.

105 Audizione del Presidente del Garante per la protezione dei dati personali A. Soro sugli schemi di decreti legislativi attuativi del c.d. Jobs Act presso la Commissione Lavoro della Camera dei Deputati (9 luglio 2015) e la Commissione Lavoro del Senato (14 luglio 2015). http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4119045.

106 A. DEL NINNO, *In vigore la riforma dell'art. 4 dello Statuto dei lavoratori sui controlli a distanza: il decreto legislativo 14 settembre 2015 n. 151, privacy dei lavoratori e nuove regole*, *Diritto e Giustizia*, 2015, 11.

I principi appena considerati hanno evidentemente portata generale e devono essere calati, nel dettaglio, nell'ambito del rapporto di lavoro. Appare necessario dunque analizzare le altre fonti alle quali l'art. 4, comma 3, rimanda attraverso il riferimento al Codice della privacy, ovvero i provvedimenti del Garante, in particolare quello relativo al corretto impiego della posta elettronica ed Internet nell'ambito lavorativo.

9. Le Linee guida del Garante della privacy in materia di posta elettronica e Internet.

Come anticipato, se il Codice della privacy contiene norme e principi generali suscettibili delle più svariate applicazioni, le norme esecutive sono rappresentate dai provvedimenti che il Garante ha emanato in materia nell'esercizio dei poteri riconosciutigli dalla legge. In questa sede, si fa riferimento, in particolare, al provvedimento generale del 1° Marzo 2007 recante le Linee guida per posta elettronica e Internet[107].

L'esigenza di una disciplina particolareggiata e puntuale nasce da alcune considerazioni preliminari. In primo luogo, è necessario valutare la posizione e le conseguenti esigenze del datore di lavoro, che non solo ha la necessità di assicurare la funzionalità degli strumenti che permettono l'impiego di Internet e della posta elettronica da parte dei lavoratori nello svolgimento della loro prestazione lavorativa, in un'ottica di massimizzazione dei risultati, ma ha altresì l'interesse e l'obbligo di garantirne il corretto impiego, anche per prevenire utilizzi illeciti che possono essere per il datore stesso fonte di responsabilità. Il datore di lavoro, dunque, dovrà adottare tutte quelle misure di sicurezza che si rivelano necessarie ad assicurare l'utilizzabilità e l'integrità tanto dei sistemi informativi quanto dei dati tramite il loro uso registrati.

All'esigenza di prevenzione e monitoraggio del datore di lavoro si contrappone la necessità di tutelare i lavoratori interessati ed impiegati nell'utilizzo dei predetti strumenti, i quali ultimi consentono controlli capillari ed invasivi della sfera del singolo, potendo essi estendersi all'acquisizione di dati personali, anche sensibili, relativi a lavoratori o terzi, identificati o identificabili[108].

---

107 Esse rispondono all'esigenza di "prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet". Premessa (Punto 1.1) alle Linee guida per posta elettronica e Internet, delibera n. 13/2007.

108 A questo riguardo, il Garante riconosce che la legittima facoltà del datore di lavoro di controllare il corretto impiego da parte dei lavoratori degli strumenti propri dell'azienda debba trovare una limitazione nell'esigenza di proteggere la dignità e la riservatezza del dipendente, impedendo la conoscenza di informazioni relative a dati personali sia del lavoratore che di terzi che con questi vengono in contatto. Punto 4 delle Linee guida. Così anche I. ALVINO,

Nel tentativo di contemperare le esigenze delle contrapposte parti contrattuali, il Garante, anzitutto, le invita al rispetto dei principi di correttezza e trasparenza: il datore di lavoro dovrà dotarsi di un regolamento interno (la c.d. *policy* aziendale) opportunamente pubblicizzato ed aggiornato, con l'indicazione chiara e particolareggiata delle corrette modalità di utilizzo degli strumenti messi a disposizione e della possibilità, misura e modalità dei controlli[109].

Con riferimento alla navigazione Internet, vari sono gli accorgimenti che il Garante individua al fine di assicurare la tutela del lavoratore e, nel contempo, di evitare il pericolo dell'inutilizzabilità dei dati raccolti dal datore di lavoro.

Anzitutto, viene proposta l'individuazione di un elenco di siti Web considerati, a priori, pertinenti alla prestazione che il lavoratore deve rendere nell'esecuzione del suo contratto di lavoro e, nel contempo, potranno essere inclusi in una sorta di *black list* quelli che, al contrario, da essa esulano. La misura in questione, tuttavia, appare di incerta applicazione. Deve infatti considerarsi l'attuale realtà del Web, la molteplicità dei siti e la loro continua ed esponenziale proliferazione, che preclude una preventiva ed esaustiva elencazione o categorizzazione (si potrebbe persino giungere alla paradossale ipotesi per cui il lavoratore, timoroso di incorrere in una violazione della *policy* interna e nella conseguente sanzione, "paralizza" o, comunque, non massimizza la propria attività lavorativa evitando la navigazione relativamente ad un sito collegato alla propria prestazione ma, non incluso nell'elencazione redatta dall'azienda). Più utile e praticabile appare un altro accorgimento, ovvero l'utilizzo di *software*, di filtri o di sistemi che impediscano la possibilità di mettere in atto determinate operazioni, come, per esempio l'accesso a siti (o, più verosimilmente, categorie di siti) prestabiliti, il *download* di *file* o programmi caratterizzati da elementi comuni per tipologia o dimensioni[110].

L'articolo 4 dello Statuto dei lavoratori alla prova di internet e della posta elettronica, *Dir. delle rel. indu.***,** 2014, 1007.

109 Per A. DEL NINNO i datori di lavoro (privati e pubblici) devono assolutamente aggiornare ed integrare il disciplinare interno, il quale non dovrebbe riguardare solo la posta elettronica ed Internet, ma anche tutti gli strumenti e le risorse informative ed informatiche, poiché tutti strumenti affidati all'uso del lavoratore, al fine di allinearlo con la modifica apportata all'art. 4 Stat. Lav. *In vigore la riforma dell'art. 4 dello Statuto dei lavoratori sui controlli a distanza: il decreto legislativo 14 settembre 2015 n. 151, privacy dei lavoratori e nuove regole*, *Diritto e Giustizia*, 2015, 14.

110 Il datore di lavoro, per ridurre il rischio di usi impropri della navigazione in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. In particolare, il datore di lavoro può adottare una o più delle seguenti misure: individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa; configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni (accesso a determinati siti o categorie di essi, *upload* o *download* di *file* non attinenti all'attività lavorativa); trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di

In questo senso, il Garante richiama espressamente il principio di necessità, di cui all'art. 3 Codice della privacy, applicandolo in ambito giuslavoristico. Innanzitutto, il datore di lavoro è, in tal modo, vincolato all'impiego di quei soli strumenti di controllo strettamente necessari, onde minimizzare l'accesso ai dati ricavati ed, inoltre, è obbligato ad avvalersi di misure organizzative e tecnologiche che siano idonee a prevenire l'utilizzo improprio di Internet e della posta elettronica, riducendo in tal modo l'eventualità di controlli successivi[111].

Per di più, il Garante esplicita la regola della graduazione dei controlli, per la quale il datore di lavoro potrà sì utilizzare le informazioni registrate al fine di verificare l'origine e la causa di un'eventuale anomalia, ma il controllo dovrà basarsi, preliminarmente, su dati aggregati, cioè quelli riferiti ad un'insieme di lavoratori impiegati nel medesimo settore o che si avvalgono dei medesimi strumenti e, solo successivamente, permanendo un uso improprio di Internet o della posta elettronica, potranno essere effettuati controlli individuali e specifici[112].

Le informazioni raccolte, in ogni caso, potranno essere conservate per il solo tempo necessario a perseguire le finalità esplicitate, ovvero quelle di organizzazione, produzione e sicurezza legislativamente determinate. I tempi di conservazione dei dati possono essere eccezionalmente prolungati qualora ciò sia imposto da esigenze tecniche o di sicurezza particolari, dalla rilevanza e non sostituibilità del dato in relazione all'esercizio o alla difesa di un diritto in giudizio o, ancora, dalla circostanza che l'informazione debba essere tutelata o consegnata al fine di soddisfare una specifica richiesta avanzata dall'autorità giudiziaria[113].

In relazione alla graduazione dei controlli, il Garante richiama i principi di pertinenza e non eccedenza, stabilendo il divieto di eseguire controlli prolungati, costanti o indiscriminati e sottolinea l'opportunità di intervenire con accorgimenti tecnici volti a riservare quale risorsa ultima l'effetuazione di controlli individuali[114].

---

utenti mediante loro opportune aggregazioni; eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza. Punto 5.2.

111 Punto 5.2, lett. a.

112 Punto 6.1

113 Punto 6.2. Per ciò che concerne i sistemi *software*, questi devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet ed al traffico telematico, la cui conservazione non sia necessaria. In assenza di specifiche esigenze tecniche o di sicurezza, la conservazione temporanea dei dati deve essere giustificata da una finalità determinata ed, in ogni caso, limitata al tempo necessario a raggiungerla.

114 Punto 6.1

Infine i principi di correttezza e trasparenza fanno sì che il datore di lavoro sia tenuto a dare adeguata informazione ai propri dipendenti circa le modalità mediante le quali i controlli vengono esercitati[115].

Le contrapposte esigenze appena analizzate si manifestano in maniera ancora più evidente e, altresì, problematica in relazione all'impiego della posta elettronica. Alla base della regolazione di tale mezzo, infatti, sta un diritto specifico e costituzionalmente tutelato dall'art. 15 Cost.[116]

L'esigenza del datore di lavoro a che tale mezzo venga utilizzato in modo corretto, ovvero per l'esercizio dell'attività lavorativa e non già a fini (anche) personali, si scontra così con un limite spcifico inerente a quelli già in precedenza individuati (tutela della libertà, dignità e riservatezza del lavoratore). Da qui, l'intervento e gli accorgimenti del Garante, diretti a individuare il giusto equilibrio tra le contrapposte esigenze.

Viene segnalata anzitutto l'opportunità che il datore di lavoro metta a disposizione indirizzi di posta elettronica condivisi tra più lavoratori. In tal modo, da un lato, verrebbero evitate tutte quelle difficoltà connesse all'eventuale assenza del singolo lavoratore in relazione alla necessità che la sua posta elettronica "personale" (o meglio, individuale) venga consultata da altri, dall'altro, non sorgerebbero problematiche di controlli su base individuale.

Con riguardo alla circostanza che il lavoratore sia assente, viene prospettata la possibilità di impostare sistemi di risposta automatica alle *e-mail*, attraverso i quali, in caso di lontananza programmata dal lavoro, il mittente possa essere informato della circostanza o, ancora, possa essere indirizzato verso un altro soggetto/ufficio della struttura lavorativa. Per il diverso caso di assenza imprevista, il Garante introduce la figura, non poco discussa, del "fiduciario", da individuarsi in quel lavoratore che viene delegato in via preventiva dall'interessato assente a consultare e selezionare i messaggi di posta elettronica di cui il datore di lavoro può prendere visione[117]. Tuttavia, pur comprendendo la volontà del Garante di tutelare il lavoratore in modo adeguato, si rileva come allo stesso pare essere attribuito un potere più vasto e, forse, ingiustificato, di quello del datore di lavoro, il quale ultimo non può che affidarsi al controllo e alla selezione operata dal fiduciario[118]. Inoltre, l'accorgimento si rivela essere di difficile applicazione, si pensi, ad esempio, al semplice caso in cui il lavoratore si assenta per malattia improvvisa, coincidente con quella del delegato.

---

115 Punti 3.1, 3.2, 3.3, per i quali inoltre è previsto l'onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli.

116 Si ricorda che in base all'art. 15 Cost. la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili e la loro limitazione può avvenire soltanto per atto motivato dall'autorità giudiziaria con le garanzie stabilite dalla legge.

117 Punto 5.2, lett. b.

118 E. BARRACO, A. SITZIA, *Potere di controllo e privacy*, Wolters Kluwer, Milano, 2016, 39 ss.

Più praticabile ma, nel contempo, contraddittoria appare l'attribuzione al lavoratore, accanto all'indirizzo di posta elettronica ad uso esclusivamente lavorativo, di un indirizzo personale e, dunque, privato. Da un lato, l'accorgimento eviterebbe tutte quelle problematiche connesse alla necessità di contemperare esigenze datoriali e tutele di *privacy* del lavoratore, dall'altro, posta la consapevolezza delle difficoltà di separare sfera lavorativa e sfera personale derivata dall'utilizzo e dallo sviluppo della tecnologia, si giunge ad un risultato bizzarro, ovverosia quello di fornire al lavoratore non solo lo strumento di lavoro ma, altresì, uno strumento privato e personale che può distogliere il lavoratore dalla sua prestazione e sul quale, nel contempo, il datore di lavoro non può esercitare controllo alcuno.

Alla luce di tali Linee guida, infine, il Garante vieta il trattamento di dati personali operato mediante l'utilizzo di *hardware* o *software* preordinati all'analisi sistematica ed analitica di indirizzi Web e messaggi di posta elettronica ovvero dei caratteri inseriti mediante tastiera, che consentirebbero comunque di risalire ai siti visitati o al contenuto delle *e-mail* inviate e ricevute. Nel contempo, viene proibito il controllo occulto dei *personal computer* affidati al lavoratore nell'esercizio della sua attività lavorativa[119].

Si rileva come, nonostante le direttive e gli accorgimenti del Garante, la materia relativa ad Internet ed alla posta elettronica non sia di facile regolazione. Oltretutto, le suddette Linee guida, che configurano l'unico atto, nel loro genere, contenente specifiche regole sui controlli datoriali, andrebbero opportunamente aggiornate, poiché si limitano alla previsione di disposizioni inerenti unicamente all'impiego della posta elettronica e di Internet, laddove, invece, occorrerebbe un intervento integrativo alla luce della modifica apportata all'art. 4 Stat. Lav. e del continuo sviluppo ed impiego di mezzi tecnologici e informatici in ambito lavorativo[120].

A questo riguardo ha provveduto il Garante, per il momento, attraverso l'emanazione di opportuni Provvedimenti, i quali hanno ad oggetto proprio il trattamento dei dati personali effettuato mediante posta elettronica, Internet ed altri strumenti di lavoro[121].

---

119 Prescrizione n. 3 delle Linee guida.

120 Si ricorda il suggerimento di A. DEL NINNO che esorta il datore di lavoro ad apportare l'opportuno aggiornamento del disciplinare interno facendo riferimento a tutti i nuovi mezzi tecnologici ed informatici impiegati dal lavoratore nello svolgimento della sua prestazione. Nota 109.

121 Cfr. anche Provv. del Garante n. 303 del 13 luglio 2016, inerente al trattamento di dati personali dei dipendenti mediante posta elettronica e altri strumenti di lavoro. Qui, il Garante ha vietato ad un'università il monitoraggio massivo delle attività in Internet dei propri dipendenti. Il caso era sorto per la denuncia del personale tecnico-amministrativo e docente, che lamentava la violazione della propria *privacy* e il controllo a distanza posto in essere dall'università. L'Autorità ha rilevato che i dati raccolti fossero chiaramente riconducibili ai singoli utenti, anche grazie al tracciamento puntuale degli indirizzi IP e dei Mac *Address* (identificativo *hardware*) dei pc assegnati ai dipendenti e, dunque, che il

Da ultimo è stato emanato il Provvedimento n. 547 del 22 dicembre 2016, con il quale il Garante ha affermato che il datore di lavoro non possa accedere in maniera indiscriminata alla posta elettronica o ai dati personali contenuti negli *smartphone* in dotazione al personale. Si tratterebbe a tutti gli effetti di un comportamento illecito, in quanto la società può solo conservare tali dati per la tutela dei diritti in sede giudiziaria. Inoltre è affermato che il datore di lavoro, pur avendo la facoltà di verificare l'esatto adempimento della prestazione professionale ed il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, debba in ogni caso salvaguardarne la libertà e la dignità, attenendosi ai limiti previsti dalla normativa. Salvo restando il fatto che i lavoratori debbano essere sempre informati in modo chiaro e dettagliato sulle modalità di utilizzo degli strumenti aziendali e su eventuali verifiche[122].

10. L'utilizzabilità dei dati raccolti a fini disciplinari. Il caso Barbulescu v. Romania.

In seguito alla riforma apportata dal d.lgs. 151/2015, la disciplina della *privacy* e lo Statuto dei lavoratori interagiscono in modo tale da diventare l'una condizione di legittimità di aspetti, quali l'esercizio del potere di controllo datoriale e l'utilizzo delle informazioni così raccolte, normati dall'altro. Affinchè il datore di lavoro possa legittimamente utilizzare i dati raccolti, mediante gli strumenti di lavoro o di registrazione degli accessi e delle presenze (comma 2), a tutti i fini connessi al rapporto di lavoro, anche disciplinari, dovrà rispettare la disciplina della *privacy* e, nel caso in cui si tratti di dati ricavati attraverso gli strumenti dai quali derivi anche la possibilità di un controllo a distanza dell'attività lavorativa (comma 1), dovrà raggiungere altresì l'accordo con le rappresentanze sindacali o ottenere l'autorizzazione amministrativa, a meno che in tali atti non se ne escluda esplicitamente l'utilizzabilità[123].

---

relativo trattamento non fosse conforme alle indicazioni delle norme in materia di *privacy*. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5408460.

122 Nel caso di specie era stato rilevato che il titolare poteva persino accedere da remoto – non solo per attività di manutenzione – alle informazioni contenute negli *smartphone* in dotazione ai dipendenti (anche private e non attinenti allo svolgimento dell'attività lavorativa), di copiarle o cancellarle, di comunicarle a terzi violando i principi di liceità, necessità, pertinenza e non eccedenza del trattamento. Nel Provvedimento è chiaramente espresso che, in tal caso, la società, in qualità di titolare, avesse effettuato (e continuasse ad effettuare) operazioni di trattamento di dati personali riferiti al reclamante, nonché ad altri dipendenti, sia in costanza del rapporto di lavoro che successivamente alla sua cessazione, le quali risultano per alcuni profili non conformi alla disciplina in materia di protezione dei dati personali. http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/5958296

123 Secondo il Presidente A. SORO la possibilità di controllo dell'attività lavorativa e la conseguente utilizzabilità, anche a fini disciplinari, dei dati così acquisiti è, ad oggi, un effetto naturale del contratto, in quanto discende naturalmente dalla costituzione del rapporto di lavoro. Intervento di A. SORO, Presidente del Garante per la protezione

Il licenziamento disciplinare potrà essere disposto, ad esempio, a fronte delle informazioni ottenute tramite i monitoraggi effettuati attraverso gli strumenti di controllo a distanza o sugli strumenti di lavoro affidati al dipendente o sulla rete locale aziendale o sulla rete Internet o, ancora, sualla casella di posta elettronica a lui fornitagli[124]. Il motivo di tale licenziamento si individua nella rottura del rapporto di fiducia intercorrente tra le parti nel rapporto di lavoro, determinata dalla violazione di specifici divieti espressi dal datore ed adeguatamente divulgati.

A questo riguardo, si propone il caso, deciso dalla Corte europea dei diritti dell'uomo, relativo ad un licenziamento comminato in virtù delle informazioni ottenute mediante controlli effettuati a distanza, in particolare effettuato sulla casella di posta elettronica aziendale.

Il 12 gennaio 2016 è stata depositata a Strasburgo la sentenza *Barbulescu v. Romania*[125] che, pur riconoscendo il controllo operato sulla *e-mail* aziendale come violazione del diritto alla vita privata di cui all'art. 8 CEDU, ha ammesso la possibilità di controlli, necessari e limitati, in presenza di un divieto esplicito e consapevole. La sentenza, come si vede, affronta la delicata questione del controllo a distanza operato mediante gli strumenti indispensabili all'esercizio della prestazione lavorativa e della sua inevitabile interferenza con la necessità di tutelare la libertà e dignità del lavoratore e, nello specifico, il suo diritto alla riservatezza.

A seguito del monitoraggio effettuato sulla casella di posta elettronica del dipendente[126], il datore di lavoro ha accertato l'utilizzo dell'*account* assegnatogli a scopi personali, durante l'orario di lavoro, sebbene specifiche *policy* aziendali disponessero esplicitamente il divieto di un tale impiego del mezzo e sebbene il soggetto ricorrente fosse stato debitamente informato delle suddette *policy*, relative all'uso degli strumenti di lavoro a scopi personali, al momento dell'assunzione. A ciò era conseguito il licenziamento del soggetto, il quale, dopo averlo impugnato in primo e secondo grado (che hanno affermato la legittimità della decisione presa dal datore di lavoro), ha adito la Corte di Strasburgo, lamentando la violazione del suo diritto alla riservatezza della sua vita privata e della sua corrispondenza, tutelato dall'art. 8 della CEDU, in particolare voleva gli fosse riconosciuta la

---

dei dati personali ("L'Huffington Post", 8 settembre 2015), http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/4235378

124 Sono comunque previsti limiti al potere disciplinare del datore di lavoro, contenuti sia nell'art. 2106 c.c., che ha introdotto la regola della proporzionalità della sanzione all'infrazione, e sia nell'art. 7 Stat. Lav. che ne ha procedimentalizzato l'esercizio. In particolare, quest'ultima norma ha introdotto il principio di legalità (oltre che del contraddittorio), per cui il codice disciplinare aziendale debba indicare le infrazioni e le sanzioni ad esse corrispondenti. G. SANTORO-PASSARELLI, *Diritto dei lavori*, Giappichelli, Torino, 2013, 262.

125 Caso n. 61496/08- Barbulescu v. Romania, sent. ECHR 013 (2016) del 12 gennaio 2016.

126 Monitoraggio effettuato per scopi lavorativi (la presa d'atto di comunicazioni effettuate con i clienti) e non effettuato sull'attività lavorativa.

sua c.d. "aspettativa di *privacy*" nell'impiego della casella di posta elettronica fornitagli dal datore di lavoro per scopi altresì personali.

I giudici di Strasburgo hanno riconosciuto il coinvolgimento, nella fattispecie concreta, della norma invocata, sulla base di un'interpretazione estensiva del concetto di *privacy* e hanno successivamente indagato se il diritto del lavoratore alla vita privata dovesse ritenersi scalfito dal contrapposto interesse datoriale o se, al contrario, fosse stato trovato il giusto bilanciamento tra le due opposte esigenze[127].

Nel diritto, la Corte ha voluto ribadire un principio fondamentale, ossia quello per il quale la lecita sorveglianza del luogo di lavoro e del lavoratore non deve prescindere dal rispetto della sfera privata delle persone in esso coinvolte. Per tale ragione, nel porre in essere il controllo, il datore di lavoro deve necessariamente rispettare i parametri di trasparenza, necessità, equità e proporzionalità.

Tuttavia, nel caso in questione, i giudici di Strasburgo hanno ritenuto che le modalità attraverso le quali era stato accertato il comportamento del dipendente, contrario ai doveri del suo impiego, fossero state necessarie e proporzionate. Nessuna violazione dell'art. 8 della Convenzione poteva dunque affermarsi, in quanto era stato fatto emergere che il dipendente, pur edotto delle *policy* aziendali, aveva perpetrato il comportamento scorretto e che, nel rispetto dei principi di necessità, proporzionalità e finalità, di cui si avvale, ovviamente, anche la normativa europea sulla *privacy*[128], il controllo delle *e-mail* si configurava quale prassi residua di verifica del corretto adempimento delle mansioni da parte del lavoratore e di un suo corretto impiego di Internet e della posta elettronica, al fine di prevenire danni all'azienda[129].

La sentenza, che a prima vista pare aprire le porte ad uno smisurato controllo datoriale sugli strumenti impigati per lo svolgimento dell'attività lavorativa, porta, in realtà, all'affermazione dell'importante confine ad esso posto dalla necessità che questo sia proporzionato e non eccedente la finalità di verifica dell'adempimento contrattuale. Inoltre, la sentenza rileva che è dovere del datore di lavoro informare opportunamente i suoi dipendenti delle corrette condizioni di utilizzo dello strumento, in questo caso della casella di posta elettronica aziendale, delle modalità di controllo effettuate per fini legittimi e delle eventuali conseguenze disciplinari a cui si va incontro in caso di violazione di tali disposizioni.

---

127 A. STANCHI, *Consultabile la posta elettronica del dipendente sull'e-mail aziendale*, *Guida al Lavoro*, n. 6, 2016, 41-42.

128 Raccomandazione R(2015)5 del Consiglio d'Europa e Regolamento UE 2016/679.

129 Inoltre i controlli non erano stati ritenuti massivi ed erano stati ritenuti giustificati anche in ragione di fondati sospetti di inefficienza lavorativa. Controlli, tra l'altro effettuati solo sulla posta elettronica e non su altri strumenti di lavoro, proprio nella convinzione che tale mezzo venisse impiegato esclusivamente a fini lavorativi. G. MARCHESI, *Mail aziendale e messaggi privati: la sentenza CEDU*, 2016, http://glob.press/attualita/privacy-ed-email-aziendali/.

Sono così ribaditi quei principi che governano la materia giuslavoristica e di trattamento dei dati personali nell'ambito del nostro ordinamento.

Anche qui si rileva come la *privacy* del dipendente, nell'ambito del rapporto di lavoro, sia sì un diritto fondamentale, ma non anche assoluto. Esso deve infatti essere bilanciato con le contrapposte esigenze datoriali, meritevoli anch'esse di considerazione e tutela. È infatti un diritto del datore di lavoro quello di accertarsi che gli strumenti forniti al dipendente per l'esercizio della prestazione lavorativa vengano impiegati nel modo corretto, a maggior ragione se gli stessi mezzi possono essere utilizzati al di fuori dell'ambito lavorativo strettamente inteso, quindi per fini personali. In tale contesto deve però considerarsi l'aspettativa (legittima) di *privacy* su cui il lavoratore potrebbe fare affidamento in relazione alle comunicazioni personali effettuate mediante strumenti aziendali. Tale aspettativa, tuttavia, potrebbe essere messa in dubbio sulla base del semplice rilievo che la *e-mail* aziendale venga fornita al lavoratore come mezzo esclusivamente finalizzato ad adempiere e massimizzare la propria prestazione lavorativa.

Proprio in virtù di tali rilievi, appare necessaria una preventiva, chiara e pubblicizzata regolamentazione interna degli strumenti di lavoro che consentono, altresì, il controllo, la registrazione e il trattamento dei dati personali del lavoratore. Il datore di lavoro potrà così chiarire in maniera particolareggiata ed esaustiva le modalità attraverso le quali i mezzi dati in dotazione devono essere utilizzati e i limiti entro i quali deve essere mantenuto il loro utilizzo e, al contempo, il lavoratore, messo a conoscenza di tale regolamentazione, non avrà scusanti in caso di violazione dei divieti ed inadempimenti contrattuali.

11. La protezione dei dati personali nell'ambito lavorativo. Il Regolamento UE 2016/679.

La materia della *privacy* è stata regolamentata non solo a livello interno ma, altresì, a livello europeo, dimensione alla quale la legislazione nazionale si è sempre conformata in maniera aderente ai principi ed alla disciplina ivi espressa. Dunque, a partire dalla spinta normativa europea sono stati emanati, nel tempo, provvedimenti finalizzati ad un unico obiettivo, ossia quello di delineare una tutela efficace ed aggiornata al trattamento dei dati personali e sensibili, i quali sono sovente oggetto di pericolo in un momento storico, come quello attuale, caratterizzato da un'evoluzione tecnologica rapida ed in continua espansione, che non può essere più valutata se non, anche, in relazione al fenomeno della globalizzazione[130].

130 Nell'ambito della protezione dei dati personali, la rivoluzione tecnologica ed il cambiamento delle dinamiche economiche e sociali hanno avuto quale conseguenza il realizzarsi di trasferimenti e scambi dei dati personali all'interno dell'Unione tra gli Stati membri o anche verso Paesi terzi. Tale evoluzione ha richiesto un quadro più solido e coerente in materia di protezione e trattamento dei dati a livello europeo, al fine di apportare quella fiducia tale da

Proprio l'esigenza di assicurare una regolamentazione della materia coerente ed uniforme all'interno degli Stati membri dell'Unione, al fine di evitare disparità di trattamento che possano rendere difficoltosa la circolazione di dati personali nel mercato interno[131], ha spinto il Parlamento Europeo ed il Consiglio ad emanare il Regolamento 679/2016, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016 e destinato a sostituire, abrogandola[132], la Direttiva 95/46/Ce[133]. Esso si inserisce all'interno di quello che, insieme alla Direttiva 680/2016[134], viene definito il "Pacchetto europeo protezione dati".

Il Regolamento, entrato in vigore il 25 maggio, verrà applicato a decorrere dal 25 maggio 2018, con lo scopo di assicurare un livello coerente ed elevato di protezione delle persone fisiche e di rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, rendendo il livello di protezione dei diritti e delle libertà delle persone fisiche, con riguardo al trattamento di tali dati, equivalente in tutti gli Stati membri[135]. *Medio tempore*, gli Stati membri dovranno adeguare la propria normativa interna ai principi contenuti in tale provvedimento.

Per quanto riguarda l'Italia, esso andrà a sostituire la disciplina contenuta nel d.lgs. 196/2003. Tuttavia, il Regolamento non rappresenterà l'unica fonte di disciplina della materia *privacy*, poiché, è previsto, che le autorità dei singoli Stati membri (per l'Italia, il Garante) potranno integrarlo, regolarne aspetti specifici o, ancora, introdurre linee guida di settore[136].

---

consentire lo sviluppo dell'economia digitale nel mercato dell'Unione. Tutto ciò sempre nell'ottica per la quale la libera circolazione dei dati personali nell'Unione non debba essere limitata né vietata per motivi inerenti alla tutela dei suddetti dati ed al loro trattamento. Considerando 6 e 7 e art. 1.3 Reg. UE 2016/679.

131 Nel Considerando 10 del Regolamento è esplicitato l'obiettivo di un'applicazione coerente ed omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione.

132 Solo a far data dal 2018, le norme contenute nella direttiva 95/46/CE risulteranno abrogate ed i riferimenti alla stessa si intenderanno come riferiti al nuovo Regolamento. Art. 99 Reg. UE 2016/679.

133 La Direttiva era stata introdotta in una fase storica non ancora caratterizzata da una massiva diffusione dei *social network*, dei sistemi di conservazione dei dati su *cloud* e dei sempre più nuovi ed aggiornati mezzi tecnologici implicanti la registrazione ed utilizzazione di informazioni personali. Tale considerazione (unita al rilievo per cui sarebbero opportune, alla luce di un progresso tecnologico costante, l'evoluzione delle modalità di raccolta e di trattamento dei dati e la risoluzione delle divergenze tra i diversi Stati membri nell'attuazione della direttiva del 1995) da anni suggeriva alla Commissione Europea un intervento regolativo del nuovo scenario attraverso un nuova disciplina della *privacy* che garantisse una più intensa tutela al diritto alla protezione dei dati personali.

134 Direttiva UE 2016/680 del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati.

135 Considerando 10 e artt. 1.1 e 1.2 Reg. UE 2016/679.

136 Considerando 8 e art. 88 Reg. UE 2016/679. Si auspica che il Legislatore italiano, nel prevedere misure appropriate e specifiche in materia e nel disporre le relative sanzioni, provveda a riconoscere effettività al principio

Dal punto di vista del contenuto, occorre preliminarmente precisare che, avendo la normativa italiana seguito il percorso europeo fin dalla Direttiva 95/46, i principi esplicitati dal nuovo provvedimento sono i medesimi che governano la disciplina interna: viene mantenuto l'obbligo di informare l'interessato circa il trattamento che verrà operato dei suoi dati, il diritto di accesso agli stessi, o, ancora, viene ribadita la necessità che venga prestato il consenso relativamente al trattamento non necessario di dati o a quello avente ad oggetto informazioni sensibili, in grado di rivelare, per esempio, le convinzioni religiose, gli orientamenti sessuali o lo stato di salute del singolo.

Per quanto riguarda poi l'ambito di applicabilità territoriale, la disciplina del Regolamento si rivolge, da un lato, a tutte quelle aziende ("titolari" del trattamento dei dati personali) che presentano uno stabilimento all'interno dell'Unione e, dall'altro, alle persone fisiche ("interessate" al trattamento dei propri dati) presenti nel territorio dell'Unione, anche qualora l'azienda titolare non abbia uno stabilimento all'interno del contesto europeo, qualora il trattamento abbia riguardo all'offerta di beni o alla prestazione di servizi ai soggetti stessi ovvero il monitoraggio del loro comportamento, sempre che quest'ultimo venga posto in essere all'interno del territorio europeo[137]. La regolamentazione non viene invece estesa alle persone giuridiche[138].

In ambito giuslavoristico, la tutela della protezione dei dati personali del dipendente definisce nuovi limiti al potere di controllo del datore di lavoro.

Un primo limite è configurato dall'obbligo di dare adeguata informativa al lavoratore e dal suo diritto di accesso al fascicolo[139] contenente i propri dati personali. Nel Regolamento l'obbligo di

---

dell'inutilizzabilità dei dati personali del dipendente illecitamente raccolti (nuovo art. 4 co.3, Tat. Lav.), principio il quale si è trovato ad essere sempre depotenziato dalla forte resistenza giurisprudenziale a riconoscere limiti all'ammissibilità in giudizio di informazioni acquisite in violazione delle norme a tutela della *privacy*. Così C. GAMBA, *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove* , LLI, vol. 2, n. 1, 2016, 5.

137 L'estensione del campo di applicazione territoriale risulta di notevole importanza per i lavoratori di società appartenenti a gruppi societari multinazionali. Essa consentirà una protezione della riservatezza dei dipendenti che lavorano o vivono nell'Unione, anche nelle ipotesi in cui titolari e responsabili (*processor*) del trattamento non avranno sedi legali, né sedi secondarie nell'UE (si ha un'eccezione nell'ipotesi di trasferimento di dati personali dall'Unione agli Stati Uniti, per la quale vale l'accordo EU-US *Privacy Shield* del 2 febbraio 2016).Il Regolamento troverà applicazione anche ai "gruppi di imprese" (ove una società è controllante e le altre controllate), per cui sarà possibile individuare l'Autorità Garante capofila nell'Autorità Garante dello Stato nel quale è presente lo stabilimento principale del titolare al trattamento (art. 4.19). In ogni caso, anche nell'ipotesi di lavoratore distaccato, le società dovranno prevedere "norme vincolanti di impresa", allo scopo di fornire un adeguato livello di protezione dei dati (art. 47).

138 Art. 3 Reg. UE 2016/679.

139 Nonostante tale diritto, nella normativa italiana, sia espressamente previsto dal d.lgs. 196/2003, per lungo tempo è stato effettivamente riconosciuto maggiomente nell'ambito dell'impiego pubblico. In ambito privato solo il Garante si era espresso sulla questione ripetutamente. Recentemente anche la Cassazione ha finalmente considerato il diritto

informativa acquista una autonoma rilevanza, anche nelle fattispecie in cui non è necessario ottenere il consenso per procedere al trattamento. Si denota, in questo modo, un capovolgimento della tradizionale prospettiva della disciplina della *privacy*, per la quale l'informativa era atto preliminare all'eventuale consenso dell'interessato al trattamento. Ora invece, secondo la nuova disciplina europea come anche nell'ambito giuslavoristico, è il fornire l'adeguata informativa al lavoratore ad essere condizione di legittimità del trattamento[140].

Un altro limite al potere di controllo e disciplinare del datore di lavoro può essere individuato nella previsione di nuove figure volte ad affiancare il titolare del trattamento nell'adempimento dei suoi obblighi e delle sue responsabilità. Si fa riferimento, in particolare, alla figura del *data protection officer* (DPO), cioè il responsabile della protezione dei dati. La sua designazione viene resa obbligatoria per tutte le aziende pubbliche nonché per quelle private in relazione alle quali il trattamento dei dati risulta particolarmente rischioso, perché, ad esempio, impone un monitoraggio continuo e sistematico dei soggetti interessati su larga scala, determinandone una profilazione[141] [142].

---

all'accesso quale vero e proprio diritto soggettivo del lavoratore, in quanto direttamente derivante dal contratto di lavoro. Secondo la Corte l'obbligo del datore di lavoro di consentire al dipendente pieno accesso a tutti i dati detenuti dal datore deriva dai generali obblighi di buona fede e correttezza che incombono sulle parti del rapporto di lavoro ai sensi degli artt.1175 e 1375 c.c. Cass., SS.UU., 4 febbraio 2014, n. 2397; Cass., sez. lav., 7 aprile 2016, n. 6775.

140 Cfr. M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, cit., 27 e C. OGRISEG, *Il Regolamento UE n.2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, LLI, vol. 2, n. 2, 2016.

141 La profilazione è quella "forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere 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 nella misura in cui ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona" (art.4.3 *bis*) Cfr. anche Considerando 58.

142 Il DPO viene concepito come una figura che, dal punto di vista strutturale-organizzativo, può presentarsi alternativamente come interna o come esterna all'azienda. Per poter svolgere le attività richieste, il responsabile della protezione dei dati deve avere un'adeguata conoscenza della normativa *privacy* e delle prassi in materia di protezione dei dati. Egli svolge i suoi compiti con autonomia e indipendenza, tra i quali: predisporre un articolato insieme di misure di sicurezza finalizzate alla tutela dei dati; informare tanto il titolare del trattamento quanto i soggetti interessati degli obblighi che discendono dal Reg. UE; presiedere alla verifica della corretta applicazione della normativa; fornire, qualora richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati; collaborare con le Autorità competenti (in Italia, il Garante); verificare la corretta applicazione della protezione dei dati fin dalla progettazione di applicativi (*privacy by design*), controllando che gli stessi abbiano impostazioni *privacy* predefinite (*privacy by default*). Art. 39 Reg. UE. Tra i suoi compiti si annovera la valutazione di impatto sulla protezione dei dati, da eseguire prima di iniziare il trattamento, qualora esso sia automatizzano o, ancora, si riferisca ad informazioni sensibili o ottenute mediante monitoraggio continuo e sistematico, dal quale derivi una profilazione. Art. 35 Reg. UE 2016/679.

Si nota come la forte responsabilizzazione del titolare del trattamento (quindi del datore di lavoro), così come delineata dal Regolamento[143], nei confronti della protezione dei dati personali dei dipendenti, andrà ad imporre una condivisione della nuova normativa a tutti i livelli, con l'acquisizione da parte dei dipendenti di nuove consapevolezze e aspettative di tutela.

Inoltre, il datore di lavoro ha l'obbligo di prestare maggiore attenzione per ciò che concerne la conservazione dei dati personali del lavoratore e le conseguenze relative all'ipotesi di cancellazione e distruzione di tali dati, che si può verificare in caso di conclusione del rapporto lavorativo. Infatti, il Regolamento prevede il "diritto di rettifica", ossia di modifica dei dati personali senza ingiustificato ritardo (art. 16, Reg. UE 2016/679) e il "diritto all'oblio", ossia di veder cancellati o deindicizzati (eliminati dai motori di ricerca) dati personali dopo un determinato periodo di tempo, fatta salva l'esistenza di motivi legittimi di conservazione (come ad esempio per rispettare obblighi di legge, per garantire diritto di cronaca o per finalità documentaristiche) (art. 17 Reg. UE 2016/679)[144] [145]. Bisogna tenere in considerazione che la previsione di questi nuovi diritti di rettifica e cancellazione dei dati, così come previsti dal Regolamento, potranno avere una rilevanza tale da garantire l'effettività della protezione dei dati personali dei dipendenti solo qualora, come già accennato[146], si provveda ad una puntuale regolamentazione anche processuale del principio dell'inutilizzabilità delle informazioni trattate in violazione della disciplina della *privacy*.

Particolari limiti e divieti sono poi previsti qualora si trattino in modo automatizzato dati riferibili al dipendente concernenti la persona fisica, al fine di analizzarne o prevederne aspetti riguardanti, ad esempio, il rendimento professionale o l'affidabilità nello svolgimento delle mansioni (cd. profilazione)[147].

---

143 Non solo l'esplicita delineazione del titolare del trattamento quale figura sul quale ricadono tutte le responsabilità inerenti al trattamento dei dati, ma anche il suo affiancamento da parte di ulteriori figure quali quella del *processor* (art. 4.8) e del *data protection officer* (artt. 37-39), determinano un ruolo di maggiore responsabilizzazione da parte del titolare.

144 Diritto configurato dalla Corte di Giustizia, a partire dalla sentenza del 13 maggio 2014, C-131/12 Mario Costeja Gonzalese e AEPD contro Google Spain e Google Inc. L'art. 17 del Reg. prevede che la cancellazione potrà essere pretesa senza ingiustificato ritardo, qualora i dati non siano più necessari rispetto alle finalità per cui sono stati raccolti ovvero se sia stato ritirato il consenso o fatta opposizione al trattamento, in assenza di motivi legittimi che lo giustifichino oppure se i dati sono stati trattati illecitamente oppure se la cancellazione è prescritta al responsabile del trattamento da un obbligo di legge.

145 Quanto alla conservazione dei dati da parte del datore di lavoro, sono altresì previsti il diritto alla limitazione del trattamento (art. 18) e il diritto alla portabilità del dato (art.20).

146 Nota 136.

147 Artt. 21,22 Reg. UE 2016/679.

Infine, si rileva come anche la nuova previsione circa la progettazione e l'impostazione predefinita[148] contribuisca in modo importante alla definizione di nuovi confini nel panorama della disciplina della *privacy*. In particolare, i concetti di *privacy by design* e *privacy by default* stanno ad indicare, rispettivamente, la messa in atto, da parte del titolare del trattamento, di quelle misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione del trattamento, e quelle misure volte a garantire che il trattamento si adempia, per impostazione predefinita, solo per quei dati necessari alle specifiche finalità che lo giustificano[149]. In altri termini, il titolare del trattamento dovrà configurare, a partire dalla fase progettuale, delle impostazioni determinate già delineate, che si conformino alla disciplina in tema di protezione dei dati personali, ciò al preciso scopo di rendere più agevole il rispetto della tutela della disciplina della *privacy* e quindi dei diritti degli interessati.

In conclusione, non si è potuto far a meno di riconoscere l'indissolubile intreccio la tra protezione dei dati personali e la tutela della persona-lavoratore nell'ambito del rapporto di lavoro, individuabile anche nella disciplina del Regolamento UE sulla protezione dei dati personali. Le nuove norme delineate a tutela della riservatezza sia puntualizzano principi già contenuti nella previgente regolamentazione e sia configurano principi che si pongono l'obiettivo di rivoluzionare il sistema di protezione della persona anche nel contesto occupazionale, all'interno della relazione lavorativa, imponendo un cambiamento di prospettiva circa il rapporto tra le parti e l'organizzazione aziendale.

12. Lo *smart working*.

Lo *smart working*, anche noto con l'espressione "lavoro agile", si è fatto negli ultimi anni sempre più spazio nello scenario lavorativo italiano. Esso ruota attorno al concetto di "agilità", che è strettamente collegato a quello di "produttività", tant'è che il lavoratore, se lasciato libero di organizzare spazi, tempi e luoghi propri di lavoro, viene reso più responsabile della prestazione che adempie e si rende disponibile a fissare degli obiettivi di produttività da raggiungenre in autonomia.

148 Art. 25 Reg. UE 2016/679.

149 Art. 25 Reg. UE 2016/679. M. SOFFIENTINI, *Protezione dei dati personali: nuovo Regolamento Ue, Diritto&Pratica del lav*., 26/2016, 1565 ss.

Precursore del lavoro agile è stato il telelavoro, regolamentato, nell'ordinamento italiano nel settore privato, a partire dall'accordo interconfederale del 9 giugno 2004[150] ed indicante un'attività di lavoro svolta fuori dei locali dell'azienda attraverso l'uso di un'apparecchiatura telematica.

Il telelavoratore si avvale di una postazione di lavoro situata nel proprio domicilio ovvero in un luogo distante dalla sede dalla quale dipende (c.d postazione remota)[151], mentre lo *smart worker*, pur sempre basando lo svolgimento della sua attività al di fuori dell'ufficio, si caratterizza per una maggiore autonomia decisionale per quanto riguarda la flessibilità dell'orario di lavoro e dei luoghi in cui si adempie.

Infatti per *smart working* si deve intendere quella forma di gestione flessibile del rapporto di lavoro, le cui modalità di organizzazione, finalizzate ad una più efficace conciliazione delle esigenze produttive con le esigenze relazionali e sociali del lavoratore, consentono una nuova considerazione di quei caratteri fondamentali che tradizionalmente connotano il rapporto di lavoro subordinato, ossia il luogo di lavoro, di norma determinato dal datore di lavoro, e l'orario di lavoro, anche questo predeterminato dal datore secondo i limiti legali e contrattuali, la cui stretta osservanza da parte del dipendente rappresenta uno dei contenuti minimi della valutazione della diligenza del suo adempimento[152].

Da fenomeno regolamentato pressocchè esclusivamente dalla contrattazione collettiva, il lavoro agile, in seguito alla sua sempre maggiore diffusione, ha assunto contorni più definiti grazie ad una sua previsione legislativa contenuta nel disegno di legge n. 2223/2016, approvato dal Senato nella seduta del 10 maggio 2017, relativo alle misure per la tutela del lavoro autonomo e alle misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato, con la dichiarata finalità di incrementare la competitività ed agevolare la conciliazione dei tempi di vita e di lavoro.

Il suddetto disegno di legge esclude che lo *smart working* possa essere qualificato quale forma contrattuale atipica, poiché esplicitamente ne descrive le modalità di esecuzione nell'ambito del rapporo di lavoro subordinato (art. 2094 c.c.), prevedendo così la responsabilità in capo al datore di lavoro della sicurezza sul lavoro e del buon funzionamento degli strumenti tecnologici rilasciati per lo svolgimento dell'attività lavorativa.

Elemento essenziale per la costruzione di tale tipologia contrattuale è l'accordo tra le parti, attraverso il quale esse gestiscono gli aspetti inerenti all'attività lavorativa, in particolare quelle

150 Con riferimento al settore pubblico, la materia è regolamentata dall'art. 4 l. 191/1998 e dal d.p.r. 70/1999. Nel settore privato, come già affermato, la disciplina è determinata dalla contrattazione collettiva, la quale si è basata su un precedente accordo quadro europeo del luglio 2002.

151 G. SANTORO-PASSARELLI, *Diritto dei lavori*, quarta edizione, Giappichelli, Torino, 2013, 460.

152 P. STAROPOLI, *Smart working e controllo sul lavoratore tramite gli strumenti di lavoro, Ipsoa Massimo Mutti-Copyright* , Wolters Kluwer, Vol. 5, 2017, 297.

modalità di esecuzione della prestazione che non presentano vincoli già predeterminati di orario e di luogo di lavoro.

Dunque, la prestazione di lavoro agile viene individuata e disciplinata mediante un accordo individuale intercorrente tra datore di lavoro e lavoratore, stipulato in forma scritta, il quale si trova a dover definire necessariamente non solo i tempi di lavoro e di riposo ed il luogo di svolgimento, ma altresì l'esercizio del potere direttivo e di controllo della parte datoriale e gli strumenti impiegati dal lavoratore nell'adempimento della sua prestazione[153].

Proprio l'utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa agile, che si compie a distanza, oltre a rappresentare un contenuto essenziale dell'accordo, pone anche la questione della corretta definizione dei limiti al suddetto potere di controllo, in una fattispecie ove il controllo sembra essere intrinseco nell'esecuzione della prestazione.

A tal proposito, il Legislatore, nel disegno di legge, ribadisce che le modalità in cui si dispiega il potere datoriale di controllo, previste nell'accordo di lavoro, devono necessariamente confrontarsi con quanto stabilito dall'art. 4 Stat. Lav., ciò proprio per evitare di comprimere eccessivamente la tutela prevista dall'ordinamento nei confronti dei diritti del lavoratore (in particolare quello alla riservatezza), in considerazione dell'attenzione che va posta nell'applicare un regime speciale relativo all'adozione di strumenti tecnologici.

La questione si pone evidente in relazione a quanto previsto dal comma secondo dell'art. 4, per il quale gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa non necessitano della procedura sindacale o autorizzativa che vincola gli strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività lavorativa.

La prima considerazione, a questo riguardo, rileva che non ogni strumento del quale il lavoratore disponga o che gli sia stato assegnato dal datore di lavoro, dal quale possa derivare un controllo a distanza sulla sua attività, possa considerarsi strumento di lavoro *stricto sensu*, ossia strumento impiegato necessariamente e causalmente nell'adempimento della prestazione lavorativa[154], con la conseguenza che non ogni strumento impiegato possa ritenersi sottratto al regime generale dell'accordo o autorizzazione preventivi.

La seconda considerazione muove dall'opportunità di ricercare un equilibrio tra la connotazione della flessibilità prevista per gli orari ed i luoghi di lavoro, realizzata attraverso una maggiore

153 Artt. 15, 16, 18 ddl. 2223/2016.

154 Lo strumento di lavoro può essere qualificato come quello che il lavoratore impieghi direttamente per lo svolgimento della prestazione ed implica una sua configurazione quale mezzo funzionale alla corretta esecuzione della mansione oggetto del contratto, laddove lo strumento, da un lato, necessariamente serva al lavoratore per l'adempimento dell'obbligazione contrattuale, dall'altro, si dimostri utile a soddisfare l'interesse del datore di lavoro a ricevere la prestazione. Per la distinzione tra strumento di controllo e strumento di lavoro si rimanda al par. 6.

autonomia di determinazione concessa al lavoratore ed il singolare impiego di strumenti tecnologici, e l'esercizio del potere datoriale di controllo.

Tale equilibrio è da ricercarsi nell'accordo di lavoro stipulato tra le parti, il quale disciplina l'esecuzione della prestazione lavorativa, determina le forme di esercizio del potere direttivo e di controllo ed individua gli strumenti utilizzati dal lavoratore, tutto ciò nel rispetto di quanto previsto dall'art. 4 Stat. Lav. Inoltre, è sempre tramite l'accordo che il lavoratore dovrà essere messo a conoscenza delle modalità d'uso degli strumenti e di effetuazione dei controlli. L'adeguata informazione ed il rispetto della disciplina della *privacy* rivestono il ruolo di condizione per l'eventuale utilizzazione (a tutti i fini connessi al rapporto di lavoro) dei dati raccolti attraverso gli strumenti di controllo preterintenzionale o di rendimentto della prestazione lavorativa, ai sensi del terzo comma della norma statutaria.

Infine la materia, così come disciplinata dal disegno di legge, fa emergere un'altra importante questione, ossia quella inerente al diritto alla disconnessione del lavoratore.

Tale questione viene in risalto laddove si constati che si sta assistendo da diversi anni ad un mutamento radicale degli elementi centrali del rapporto di lavoro subordinato e della loro concezione dal punto di vista culturale, in una visione del tempo e del luogo di lavoro quali concetti più fluidi, che hanno favorito il consolidarsi di un sistema ove la vita privata si intreccia e si confonde con la vita lavorativa, determinando l'incapacità concettuale di separare il "tempo di lavoro" dal "tempo libero"[155]. È noto che ormai oggi il lavoratore che utilizza, per lavoro (ma non solo), la tecnologia informatica del comune *smartphone* o di un qualsiasi altro dispositivo tecnologico, venga bombardato di avvisi e di notifiche di ogni genere, anche inerenti all'ambito lavorativo, trovandosi così in difficoltà nello scindere la sfera personale da quella professionale, a maggior ragione se si considera che tutto questo avviene nel corso dell'intera giornata.

Per quanto la normativa espressa nel disegno di legge e, prima di essa, gli accordi collettivi abbiano affermato che la prestazione lavorativa resa a distanza debba essere mantenuta entro i confini del normale orario di lavoro concordato, tale difficoltà, anche ormai culturale (se si considera l'incalzante evoluzione tecnologica dei mezzi di comunicazione e connessione e l'assuefazione sociale a ciò), di separazione della vita privata dalla vita lavorativa complica il quadro, determinando una concreta problematicità nel ricondurre ad una dimensione prettamente giuridica la questione del tempo di lavoro (e del tempo libero), non più facilmente sussumibile nell'ambito delle norme tipiche del diritto del lavoro.

155 F. ROTONDI, *Diritto alla disconnessione del lavoratore: non è necessario "per legge"*, *Ipsoa Wolters Kluwer*, 2017,http://www.ipsoa.it/documents/lavoro-e-previdenza/rapporto-di-lavoro/quotidiano/2017/05/20/diritto-alla-disconnessione-del-lavoratore-non-e-necessario-per-legge.

In conclusione, il diritto alla disconnessione dovrebbe essere analizzato e riletto alla luce di una maggiore consapevolezza degli aspetti che l'avvento della tecnologia e delle sue implicazioni hanno apportato sia nell'ambito lavorativo quanto in quello privato e ciò sia per quanto riguarda la disconnessione che può essere riferita al compimento di attività proprie dello svolgimento della prestazione lavorativa (ad esempio, rispondere a chiamate di lavoro o a *e-mail* oltre il normale orario di lavoro), sia la disconnessione che interrompe, nel tempo libero, il controllo a distanza dell'attività lavorativa operato dal datore di lavoro.

13. Controllo a distanza e *social network*.

Particolare attenzione si vuole riservare al rapporto sussistente tra controllo a distanza del lavoratore e *social network*. Quest'ultimo è infatti diventato, nella società moderna, mezzo di comunicazione e socializzazione che, se non necessario, si presenta quantomeno come ordinario. Esso, tuttavia, in una realtà difficilmente gestibile quale è quella dell'incessante sviluppo tecnologico e della conseguente circolazione di dati, fa sorgere non poche problematiche. In ambito lavorativo, esse ineriscono altresì, o soprattutto, la tematica della sorveglianza a distanza del lavoratore.
Il controllo del lavoratore su un *social network* può attivarsi sin dalla creazione di un profilo identificativo personale (attraverso la pubblicazione sulla piattaforma di contenuti e la personalizzazione di questi) e dalla partecipazione attiva alla società virtuale. Tale adesione crea delle connessioni che a loro volta possono generare un controllo involontario, rendendo noti all'esterno frammenti di vita privata altrimenti non conoscibili.
In ambito lavorativo appare utile considerare i seguenti aspetti.
Innanzitutto, prendendo atto delle sollecitazioni e degli stimoli cui il lavoratore si sottopone, dedicando tempo ed energia alla sua vita virtuale, durante l'orario lavorativo, si pone la questione di quanto tali risorse, tempo ed energia appunto, siano sottratte all'attività lavorativa che egli è contrattualmente chiamato a svolgere. In questo caso, il lavoratore andrebbe contro il suo dovere di diligenza a cui è tenuto ai sensi dell'art. 2104 c.c., oltre che si presterebbe a violare le prescrizioni di correttezza e buona fede caratterizzanti la natura del contratto ai sensi degli artt. 1175 e 1375 c.c.
Inoltre, il lavoratore, attraverso i *social network*, potrebbe mettere in atto, al pari di quanto succede nella vita reale, azioni e comportamenti che possono cadere nell'inadempimento contrattuale o persino nell'illecito. Tali atti, virtuali, si trasformano in conseguenze reali, perseguibili e punibili. Si pensi al caso in cui il lavoratore, attraverso la pubblicazione di foto scattate nei locali dell'azienda sul suo profilo (visibile "agli amici degli amici" o "pubblico"), vada a ledere il patrimonio aziendale, il quale si compone anche di quei beni immateriali includenti l'immagine aziendale, il

know how e i segreti industriali, rompendo, in questo modo, il rapporto di fiducia che lo lega contrattualmente al datore di lavoro[156].

Tutto ciò può potenzialmente accadere poiché tali piattaforme informatiche mettono a disposizione innumerevoli funzioni tecnologiche, quali il supporto per la pubblicazione di immagini, video o commenti, un servizio di messaggistica in tempo reale (*chat*), attuano la geolocalizzazione ed individuano l'orario in cui ciascuna azione viene compiuta. Lo scopo è quello dell'interazione con altri utenti, attraverso la presentazione e lo scambio di informazioni personali, a partire dallo svelamento della propria identità, dei propri gusti (*like*), delle proprie opinioni e della propria quotidianità, la quale comporta un mescolamento tra la vita reale e la vita virtuale.

Alla luce di ciò non si può far a meno di constatare che di questa vita virtuale e delle azioni ivi messe in atto rimane traccia all'interno della suddetta piattaforma, che registra dati personali ed informazioni la cui divulgazione potrebbe comportare una compromissione della stabilità del rapporto di lavoro. Compromissione che può avere per epilogo il licenziamento del lavoratore.

É in questa prospettiva che la piattaforma del *social* diventa un utile strumento di controllo per il datore di lavoro, al fine di verificare la diligenza impiegata ed il corretto adempimento nello svolgimento della prestazione da parte del suo dipendente. Affinchè questo controllo abbia un esito, dal punto di vista giuridico, il datore si deve assicurare che le informazioni rilasciate sui *social* siano suscettibili di acquisire valore di prova nel giudizio eventualmente instaurato per contestare l'inadembimento o l'illecito.

Una doverosa premessa riguarda il periodo storico nel cui ambito viene ad inserirsi la redazione dello Statuto. Appare lampante che nel 1970 il concetto di "controllo a distanza" non poteva prevedere l'avvento dei *social network*. Il Legislatore aveva ritenuto di garantire adeguata tutela al lavoratore mediante una norma che escludeva in modo assoluto il controllo diretto sull'attività lavorativa e vincolava, attraverso l'individuazione di esigenze tipizzate e mediante la previsione di una procedura determinata, il potere di installare apparecchiature di controllo a distanza da cui potesse derivare un controllo preterintenzionale sull'attività. Fu la giurisprudenza, soprattutto di

156 Si riporta il caso richiamato nella Relazione annuale del Garante del 2010 (p. 112 su http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1819504), ove l'Autorità aveva tra l'altro affermato la legittimità dell'impiego da parte del datore di lavoro, nel giudizio instaurato in seguito al licenziamento del dibendente, di foto ricavate dal *social*, quale prova dell'illecito compiuto dal lavoratore, tale da giustificarne appunto il licenziamento. Ciò in quanto la pubblicazione delle foto era avvenuta su un profilo di ampia visibilità, poiché impostato sulla condivisione delle informazioni lì contenute agli "amici degli amici". Inoltre si riporta il caso di un lavoratore licenziato a causa della pubblicazione sul suo profilo "pubblico" di immagini che lo ritrevano fuori dall'ufficio durante l'orario lavorativo, tali da provare l'allontanamento dal luogo di lavoro e il non corretto svolgimento della prestazione. In F. IAQUINTA, A. INGRAO, *Il datore di lavoro e l'inganno di Facebook*, *Riv. it. Dir. Lav*., 2014.

legittimità, a colmare il vuoto normativo che non prevedeva in modo esplicito, tra le ragioni aziendali legittimanti il controllo, quella della tutela del patrimonio aziendale, comprensivo non solo dei beni materiali, ma anche di quelli immateriali riconducibili alla credibilità ed affidabilità dell'azienda[157]. Le informazioni ricavate all'esito dei controlli, effettuati attraverso gli apparecchi installati a norma dell'originario comma secondo dell'art. 4 Stat. Lav., non erano considerate utilizzabili per fini differenti da quelli che li avevano giustificati (come, ad esempio, per fini disciplinari), tant'è che anche gli accordi sindacali ed i provvedimenti amministrativi di autorizzazione tendevano ad escludere un tale impiego delle informazioni, prevedendo espressamente clausole di inutilizzabilità delle medesime a fini disciplinari[158]. Ma l'inutilizzabilità ai fini di prova, grazie all'opera della giurisprudenza[159], non valeva nel caso di rilevazione di fatti illeciti compiuti dal lavoratore, considerati estranei allo svolgimento della prestazione lavorativa ed idonei a ledere il patrimonio aziendale.

Per ciò che riguarda quest'ultimo aspetto, l'impiego del *social network* quale strumento di controllo a distanza, purché a scopo difensivo del patrimonio aziendale, è stato avallato dalla Cassazione, la quale ha stabilito che un tale controllo, anche se occulto, è legittimo, sempre qualora non violi i principi di buona fede e correttezza nell'esecuzione del contratto[160].

---

157 Cass., sez. lav., 23 febbraio 2012, n. 2722, ove viene messo in rilievo il diritto del datore di lavoro di tutelare il proprio patrimonio, costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico.

158 A. BELLAVISTA, *Il controllo sui lavoratori*, Giappichelli, Torino, 1995, 62.

159 In seguito al riconoscimento dei c.d controlli difensivi, i quali hanno ad oggetto non lo svolgimento della prestazione del lavoratore, ma i comportamenti illeciti lesivi del patrimonio aziendale, estranei al normale svolgimento della medesima anche se da essa occasionati. In questo modo si voleva porre in risalto l'esigenza del datore di lavoro di difendersi da tali comportamenti illeciti, la cui rilevazione, se fosse stata fatta rientrare nei vincoli di cui al vecchio comma 2 dell'art. 4 Stat. Lav., sarebbe stata ingarbugliata nei limiti e nella procedura lì prescritta. Cfr. Cass., sez lav., 23 febbraio 2012, n. 2722 e Cass., sez. lav., 4 aprile 2012, n. 5371. Par. 4, cap. 1.

160 Si fa riferimento al caso di un licenziamento per giusta causa di un dipendente, che aveva usato *Facebook* durante l'orario di lavoro. Il fatto era stato rilevato dal datore di lavoro attraverso la creazione di un profilo falso, attraverso il quale aveva interagito con il dipendente. Creazione attuata in seguito alla rilevazione di altri comportamenti negligenti da parte del dipendente, quali quello di rispondere a telefonate private, che avevano messo in pericolo la buona riuscita della regolare attività produttiva dell'azienda (la sua negligenza aveva provocato il blocco di un macchinario a cui era addetto). La Cassazione ha qui riconosciuto al datore di lavoro la legittimità di effettuare controlli difensivi occulti, anche per mezzo di personale estraneo all'organizzazione aziendale, se diretti a tutelare beni del patrimonio aziendale ovvero ad accertare la perpetrazione di comportamenti illeciti (attraverso dunque controlli *ex post*), purché ciò avvenga mediante modalità non eccessivamente invasive e rispettose della libertà, dignità e riservatezza dei lavoratori e con l'osservanza dei canoni generali di correttezza e buona fede contrattuale. Cass., sez. lav., 27 maggio 2015, n. 10995. P. SALAZAR, *Facebook e rapporto di lavoro: a che punto siamo*, *il Lav. nella giur*., 2/2016, 201; V. AMATO, *Legittimità del controllo difensivo occulto attraverso i social networks*, *il Lav. nella giur.*, 10/2015, 896 ss.

Ora, alla luce del nuovo art. 4 Stat. Lav., è prevista sia l'utilizzabilità delle informazioni raccolte a tutti i fini connessi al rapporto di lavoro (anche disciplinari), laddove si individui un'inadempimento contrattuale o un illecito tale da compromettere il rapporto di fiducia intercorrente tra le parti contrattuali[161], sia è stata mantenuta la tendenza ad attribuire loro valore di prova in un eventuale giudizio.

Un punto relativo all'ammissibilità in giudizio delle informazioni rilevate attraverso i *social* attiene alla necessità che tali informazioni siano state rese dal soggetto nei confronti di un'ampia utenza. Per rilevare ciò occorre verificare che le impostazioni inerenti al grado di pubblicità delle informazioni condivise sul profilo siano settate su una modalità pubblica o relativa alla vasta cerchia "amici di amici", poiché, in questo modo, si deduce che il soggetto avrebbe inteso renderle visibile ad una cerchia indeterminata di persone[162]. La conseguenza è che i dati così condivisi possano essere conosciuti e attinti da chiunque e quindi anche dal datore di lavoro, che, dunque, non ci si trova di fronte ad un contenuto da considerarsi riservato, proprio perché l'utente della piattaforma non ha operato quello *ius escludendi alios* rispetto alle proprie informazioni personali[163].

Tutte queste osservazioni vanno riportate alla considerazione per la quale, in seguito alla riforma dell'art. 4, l'impiego del *social network* quale strumento di controllo dovrà pur sempre rispettare la procedura di cui al nuovo comma primo e gli obblighi di cui al terzo comma. Ne deriva che il datore di lavoro, che intenda avvalersi dei *social*, quali strumenti per compiere un controllo su eventuali inadempimenti o illeciti del lavoratore nello svolgimento della sua prestazione, dovrà attenersi al rispetto dei limiti e della procedura lì normata, dunque all'obbligo di ricerca del previo accordo sindacale o autorizzazione amministrativa e all'obbligo di fornire adeguata informazione al lavoratore e di rispetto della disciplina della *privacy*[164].

---

161 Secondo la Cass., sez. lav., 9 marzo 2016, n. 4633, "il lavoratore è assoggettato non solo all'obbligo di rendere la prestazione, bensì anche all'obbligazione accessoria di tenere un comportamento extralavorativo che sia tale da non ledere né gli interessi morali e patrimoniali del datore di lavoro né la fiducia, che in diversa misura e in diversa forma, lega le parti del rapporto di durata".

162 Come affermato dal Garante nella Relazione annuale 2010, p. 112.

163 A. INGRAO, *Il controllo a distanza effettuato mediante Social network*, LLI, vol. 2, n. 1, 2016, 118.

164 Si ritengono legittimi anche se svincolati dalla procedura di cui al comma 1, art. 4 Stat. Lav. (quindi effettuati in mancanza di accordo o autorizzazione) i controlli (difensivi) diretti ad individuare illeciti extracontrattuali del lavoratore, tutt'al più occasionati dallo svolgimento della prestazione lavorativa, aventi rilevanza penale (quindi anche i controlli difensivi effettuati mediante *social network*). Ciò alla luce di una nuova ridefinizione della categoria dei controlli difensivi, resasi necessaria in seguito all'inclusione della ragione della tutela del patrimonio aziendale tra le esigenze tipizzate dal nuovo comma 1, che permettono l'impiego di strumenti di controllo a distanza preterintenzionali solo previo rispetto della procedura. Qualora non si riconoscesse legittimità ad un tale controllo difensivo, così svincolato, si arriverebbe al paradosso per il quale la registrazione di un illecito, quale il furto, non potrebbe essere

Il nuovo art. 4 Stat. Lav. influenza anche il corretto impiego del *social network* quale strumento di lavoro[165], il quale a norma del secondo comma non necessiterà della procedura di cui al primo comma, ma le informazioni tramite lo stesso rilevate saranno utilizzabili solo nel rispetto di quanto stabilito dal terzo comma. Dunque, il datore di lavoro sarà tenuto a mettere a conoscenza il dipendente, mediante apposita informativa, sia della possibile sorveglianza effettuata su quel profilo impiegato per ragioni lavorative e sia di ciò che al dipendente è concesso fare per il tramite di quel profilo e sia ciò che gli è vietato. In ogni caso, al datore non sono permessi controlli prolungati, continui ed indiscriminati[166], i quali sono da considerarsi illeciti.

Alla luce di tutto quanto detto, si può apportare una considerazione: nell'ambito lavorativo, il dipendente deve prestare cautela a tutte le azioni che pone in essere, anche quelle virtuali, mantenendo una condotta che dovrà essere ritenuta decorosa, moralmente accettabile e rispettosa delle obbligazioni assunte in sede di sottoscrizione del contratto di lavoro, a maggior ragione se si considera che tramite l'uso dei *social network*, i comportamenti eventualmente messi in atto possono avere un riverbero pubblico, laddove non si sia assunta , da parte dell'utente, un'opportuna consapevolezza sul mezzo impiegato e sulle insidie che esso cela.

L'autonomia e la tutela della *privacy* del dipendente appaiono, in ultima analisi, nelle sue stesse mani, in quanto, si ritiene che sia dall'utilizzo corretto, diligente e attento del mezzo *social* che il dipendente potrà salvaguardare il suo diritto alla riservatezza e soprattutto non compromettere il proprio rapporto di lavoro.

14. Considerazioni conclusive circa le modifiche dell'art. 4 Stat. Lav.

Dall'analisi dell'art. 4 Stat. Lav., nella sua nuova formulazione, emerge come il diritto alla riservatezza della persona-lavoratore, considerato un diritto fondamentale e meritevole della maggiore tutela possibile, debba essere necessariamente bilanciato con il potere di controllo del datore di lavoro, connaturato alla sua posizione contrattuale, giacché il potere direttivo da solo non potrebbe garantire la piena e sicura realizzazione dell'interesse a ricevere la prestazione.

Bilanciamento che deve essere effettuato, a maggior ragione, tenendo conto che, nelle dinamiche sociali e lavorative attuali, il controllo operato dal datore di lavoro si avvale di nuove tecnologie,

---

utilizzata in giudizio per giustificare il licenziamento del dipendente, qualora non realizzata attraverso uno strumento di controllo a distanza autorizzato preventivamente. Così Cass., sez. lav., 8 novembre 2016, n. 22662. Par. 4.

165 Si pensi al lavoro che può essere svolto dal punto di vista pubblicitario e promozionale dell'azienda per il tramite del *social network*, tant'è che recentemente si è delineata l'attività di *social media marketing*, svolgibile attraverso la realizzazione di un profilo apposito rappresentante l'azienda, attraverso cui il lavoratore addetto, solitamente, promuove campagne pubblicitarie e gestisce un servizio clienti *online*.

166 Provvedimento del Garante n. 547 del 22 dicembre 2016.

attraverso le quali diventa possibile addentrarsi nella vita privata del lavoratore in modo più insidioso rispetto ad un recente passato. Basti, a testimonianza di ciò, considerare che, al giorno d'oggi, lo strumento tecnologico può rivestire, contemporaneamente, la funzione di strumento necessario allo svolgimento della prestazione lavorativa e strumento di controllo al servizio del potere direttivo imprenditoriale.

Si è, quindi, ritenuto doveroso stabilire che la vigilanza attuata sul lavoratore, ancorchè necessaria nell'organizzazione produttiva, andasse mantenuta in una dimensione umana, ossia non esasperata dall'uso di tecnologie suscettibili di rendere l'opera di monitoraggio continua ed anaelastica, andando così ad eliminare ogni zona di riservatezza e di autonomia nello svolgimento del lavoro.

A tal proposito, un ruolo centrale è stato svolto dalla giurisprudenza, la quale è riuscita ad indicare di volta in volta quali fossero i limiti da porre al potere di controllo e le modalità per un suo lecito esercizio, consentendo, in tal modo, alla norma dello Statuto di confrontarsi con le innovazioni tecnologiche e di rispondere alle nuove esigenze che, nel tempo, si sono andate affermando nel mondo del lavoro.

Inoltre, appare utile rilevare come la questione della riservatezza si sia posta con urgenza in maniera evidente solo a partire dal momento in cui gli strumenti adoperati nel rapporto di lavoro si siano rivelati idonei ad acquisire informazioni personali e sensibili, le quali, grazie all'impiego delle risorse tecnologiche attuali, possono essere non solo facilmente rintracciate, ma anche memorizzate e scambiate, determinando una maggiore vulnerabilità del soggetto al controllo.

La diffusione dell'impiego della tecnologia e dell'informatica nell'ambito lavorativo ha comportato la necessaria ed auspicata modifica dell'art. 4, la quale ha determinato una revisione della disciplina dei controlli a distanza, sempre nell'ottica dell'opportuno contemperamento tra l'interesse del datore di lavoro a controllare a controllare lo svolgimento della prestazione lavorativa e l'interesse del lavoratore a vedere protetto il proprio diritto alla riservatezza.

Diritto alla riservatezza, che proprio in ragione delle modifiche normative al testo dell'articolo, è sembrato subire una flessione alla sua piena natura di diritto fondamentale.

Si fa, innnanzitutto, riferimento alla scelta legislativa di eliminare l'esplicito divieto posto, in apertura alla norma, alle operazioni aventi quale unica finalità quella del controllo dell'attività lavorativa, la quale fa sparire il divieto assoluto e l'accento su di esso posto, con tutto il significato metagiuridico che tale assolutezza porta con sé in diretto rapporto alla sensazione di una diminuita tutela del diritto del lavoratore. Ma è importante rilevare che il divieto, dal punto di vista giuridico, è pur sempre presente, seppur espresso in maniera implicita attraverso l'elencazione esclusiva dei casi in cui il controllo preterintenzionale è permesso e che probabilmente tale scelta sia stata operata in un contesto di cambiamento e di pressante attenzione (anche da parte di possibili investitori esterni in campo economico) posta sulle dinamiche legate ai poteri di forza nel rapporto di lavoro e

in una dimensione, quella attuale, dove il significato e la percezione del controllo sono radicalmente cambiati, generando un sintomo di assuefazione al controllo stesso.
In secondo luogo, si fa riferimento al fatto che gli strumenti di lavoro e di registrazione degli accessi e delle presenze prescindono dalla procedura sindacale o autorizzativa, che limita l'impiego degli strumenti preterintenzionali di controllo. Qui la necessità di non impigliare in una rete procedurale il potere di controllo del datore di lavoro è pur sempre accompagnata dalla considerazione secondo cui, pur non essendo, in questi casi, indispensabile l'autorizzazione, il datore non è libero di controllare ed esaminare i dati registrati, poiché la possibilità di impiegare lo strumento va tenuta distinta da quella di utilizzare le informazioni ricavate attraverso lo stesso.
Infatti, la parte finale della norma prevede sì l'utilizzabilità delle informazioni raccolte, attraverso l'impiego di tali strumenti (sia quelli da cui derivi anche la possibilità di controllo a distanza, sia quelli di lavoro e di registrazione degli accessi e delle presenze), a tutti i fini connessi al rapporto di lavoro (anche disciplinari), apparentemente allargando le maglie del potere di controllo datoriale, ma poi pone un' importante limite nella precisazione secondo cui i dati così raccolti siano utilizzabili solo a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e tutto ciò nel rispetto di quanto disposto dalla disciplina sulla *privacy*.
In questo modo, il Legislatore pone in risalto il diritto alla riservatezza, la cui tutela, al giorno d'oggi, è resa urgente da una realtà relazionale e lavorativa caratterizzata dall'uso massivo delle tecnologie e tiene in considerazione il fatto che, con il passare degli anni, tale diritto si sia evoluto fino a diventare il diritto per un soggetto di poter controllare tutte le informazioni raccolte da altri che lo riguardano.
A questo punto si possono svolgere due ordini di considerazioni.
La prima non può fare a meno di rilevare che, per quanto la tutela del lavoratore non sia normativamente affatto venuta meno in seguito alla nuova formulazione dell'articolo, il Legislatore abbia comunque affidato la protezione della dignità e della riservatezza del lavoratore ad una fonte normativa di carattere generale (come la disciplina in materia di protezione di dati personali), invertendo così il rapporto sistematico che nell'ordinamento esiste tra norma generale e norma speciale (la disciplina in materia di rapporto di lavoro). Il Legislatore, ponendo la disciplina dell'utilizzabilità delle informazioni registrate sotto il rassicurante e discrezionale tetto della disciplina della *privacy* (comprese le pronunce del Garante), si può ipotizzare abbia voluto togliersi la responsabilità di un'azione legislativa che potrebbe configurarsi come corrosiva nei confronti delle prerogative dei lavoratori nell'ambito della disciplina del rapporto di lavoro.
La seconda considerazione è inerente alla complessità del nuovo ruolo che viene ad assumere il datore di lavoro, alla luce del cambiamento apportato dall'imprescindibilità tecnologica e della

modifica della normativa sul controllo a distanza. Infatti il nuovo testo dell'art. 4 non ha affatto semplificato la vita del datore di lavoro, poiché si configura come opportuna una chiara e specifica consapevolezza della propria organizzazione aziendale ed una comprensione dei profili tecnici e delle loro conseguenze giuridiche. In concreto, questa è la consapevolezza che deve essere impiegata dal datore di lavoro nell'installazione ed utilizzo degli strumenti di controllo a distanza e nella rilevazione della differenza intercorrente tra strumento di controllo e strumento di lavoro e poi trasfusa nell'informativa sul trattamento dei dati (art. 13 Codice Privacy) e nell'adeguata informazione al lavoratore di cui al terzo comma dell'art. 4 Stat. Lav.

Infine, è stata considerata la disciplina del controllo a distanza in virtù dell'impiego dei *social network* ed in relazione al fenomeno dello *smart working*.

Per quanto riguarda quest'ultimo aspetto, si è potuto constatare che si tratta di una situazione, la cui dichiarata finalità è quella di incrementare la competitività ed agevolare la conciliazione dei tempi di vita e di lavoro, ove l'apparecchiatura telematica consente contemporaneamente lo svolgimento della prestazione lavorativa e il controllo della medesima, sicché si ritiene che il controllo sia intrinseco nell'esecuzione della prestazione. Di conseguenza, la disciplina delle modalità di esercizio del potere datoriale di controllo si pone quale preoccupazione esplicita del Legislatore, che ribadisce che la necessaria previsione delle stesse, nello specifico accordo intercorrente tra le parti, debba avvenire nel rispetto di quanto disposto dall'art. 4 dello Stat. Lav.

Circa il controllo a distanza effettuato mediante *social network*, ovvero mediante una piattaforma ove qualsiasi azione posta in essere da un soggetto lascia traccia, l'individuazione di dati personali e sensibili, compiuta in tale ambito, è suscettibile di determinare una compromissione della stabilità del rapporto di lavoro.

Anche in questo caso deve essere rispettato l'art. 4, con l'ulteriore complessità derivante dal fatto che l'esercizio del potere di controllo datoriale deve confrontarsi con le impostazioni di privacy selezionate dal lavoratore relative al suo profilo virtuale, essendo che è il soggetto stesso a poter decidere e quindi scegliere quale grado di pubblicità attribuire al proprio profilo attivo sul *social*.

La posizione del datore di lavoro appare aggravata, in quanto, qualora volesse avvalersi del *social network* per controllare eventuali condotte inadempienti o illecite del lavoratore o per rispondere ad una delle esigenze aziendali (organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale), dovrà rispettare le procedure sindacale ed autorizzativa previste dall'attuale primo comma dell'art. 4 e dovrà assicurarsi che il lavoratore sia stato adeguatamente informato di questa modalità di controllo a distanza a norma del terzo comma del suddetto articolo.

In conclusione, dall'analisi delle modifiche apportate dalla riforma all'art. 4, anche con riguardo a nuovi fenomeni come l'avvento dello *smart working* e dell'impiego dei *social network* , non si rileva alcun sacrificio degli interessi contrapposti del lavoratore e del datore di lavoro.

Tuttavia, ci si interroga sulle future interpretazioni che le modifiche della norma, qui trattate, potranno assumere nel corso del tempo, laddove si tenga conto non solo dei cambiamenti apportati alla società (e che ancora verranno apportati in futuro) dall'imprescindibilità che connota la diffusione tecnologica in ambito relazionale e lavorativo, ma anche della constatazione secondo cui da quella imprescindibilità e diffusione sia derivata una nuova concezione di controllo, dalla quale si è generato un sentimento di assuefazione ad esso.

Capitolo Secondo

Il controllo potenzialmente attuabile mediante strumenti informatici da parte di chiunque.

1. La vulnerabilità della tecnologia informatica e telematica al controllo.

L'evoluzione scientifica e tecnologica degli ultimi decenni ha radicalmente rivoluzionato le molteplici forme di interazione tra le persone e il modo attraverso cui le persone depositano e gestiscono le loro informazioni riservate.

Con l'avvento dei dispositivi informatici, le nuove possibilità, da questi apportate e garantite, di comunicazione e socializzazione, attraverso le piattaforme dei *social network*, di memorizzazione di grandi quantità di dati, non solo sull'*hardware*[167] dell'apparecchio, ma anche all'interno della rete Internet, grazie ai sistemi di *cloud computing*[168] e degli stessi *social* e di interazione attraverso nuove applicazioni di messaggistica (chat come *Whatsapp*, *Telegram*, *Viber*) ed attraverso il sistema VoIP[169] (*Skype*) hanno reso necessaria una considerazione circa le nuove forme di controllo.

La fruizione di mezzi di comunicazione e di supporto informatico e telematico ha assunto, in un mondo globalizzato e interconnesso come quello attuale, sempre maggior rilevanza, acquisendo man mano lo status di imprescindibilità[170], sia per quanto riguarda l'ambito strettamente personale, sia per quanto riguarda l'ambito lavorativo.

Se una persona vuole comunicare o memorizzare, al giorno d'oggi, in modo efficace e veloce, delle informazioni, di qualunque genere, farà ricorso ad un dispositivo la cui tecnologia gli garantirà e permetterà un tale risultato[171].

---

167 L'insieme delle componenti fisiche, non modificabili (alimentatori, elementi circuitali fissi, unità di memoria, ecc.), di un sistema di elaborazione dati.

168 Nel modello di *cloud computing* l'utente rinuncia al possesso di proprie risorse *hardware* e *software* ed accede a tali infrastrutture e programmi acquisendole attraverso Internet secondo i propri bisogni.

169 La tecnologia VoIP (*Voice Over Internet Protocol*) permette di instaurare conversazioni vocali (gratuite e a basso costo) tramite la rete Internet oppure anche tramite una rete privata basata sul protocollo IP (ad esempio, rete LAN - *local area network*- presente all'interno di un edificio o di un blocco di edifici).

170 Cfr. E. BRYNJOLFSSON, A. MCAFEE, i quali constatano anche la crescita esponenziale dell'evoluzione delle nuove tecnologie, considerata così intrinseca alla loro natura (ragionamento che parte dalla Legge di Moore, per cui la potenza dei calcolatori raddoppia circa ogni due anni). *La nuova rivoluzione delle macchine. Lavoro e prosperità nell'era della tecnologia trionfante*, Feltrinelli, Milano, 2015.

171 Si parla ora di "alfabetizzazione digitale", espressione con cui si intende la capacità di utilizzo dei nuovi media, attraverso la quale si ha la possibilità di partecipare in modo attivo ad una società sempre più digitalizzata. Un esempio di questa tipologia di alfabetizzazione è dato dalla capacità di saper utilizzare i nuovi strumenti TIC (*Information and Communications Technology*) per accedere all'informazione tramite i numerosi canali oggi disponibili. European

L'efficacia, la velocità e i bassi costi che caratterizzano tale modalità di gestione, trasmissione e conservazione dei dati è imprescindibilmente legata all'esponenziale diffusione dei mezzi che la consentono. Diffusione la cui conseguenza si configura nella suddetta imprescindibilità dal mezzo.
Tutto ciò si basa su un assioma di fondo, secondo il quale maggiore è la tecnologia impiegata nella comunicazione e catalogazione delle informazioni, maggiore sarà la vulnerabilità di quest'ultima al controllo, essendo che la potenzialità di controllare si è andata configurando di pari passo con lo sviluppo delle varie tecnologie impiegate nella trasmissione ed immagazzinamento dei dati.
Infatti si constata che la crescita tecnologica dei mezzi impiegati a questi fini ha visto svilupparsi, parallelamente, una variegata gamma di strumenti potenzialmente rivolti al controllo dei dati attraverso i cui mezzi sono salvati o inviati.
Le operazioni di questo genere scoprono così il fianco a molteplici ed invadenti forme di intrusione, che, a seconda del contesto nel quale ci si trova, possono essere lecite (si pensi alla captazione a fini investigativi da parte della polizia giudiziaria nell'ambito di un'indagine penale) o illecite.
Per quanto riguarda questo ultimo aspetto, si rileva che, nella pur constatata illiceità dell'atto, le ragioni che lo generano hanno radici diverse, che si proverà ad analizzare.

2. Il sistema informatico e telematico quale ambito in cui si adempie il controllo.

Possono essere oggetto di intrusione e captazione tutti i sistemi informatici e tutte le connessioni (fisse od occasionali) tra sistemi informatici e telematici, ossia tra dispositivi collegati tra loro in rete o via modem o con qualsiasi altra forma di interconnessione.
Preliminarmente, è da rilevare che tali connessioni o comuncazioni sono state assimilate a forme di comunicazioni tra persone a partire dalla l. 23 dicembre 1993, n. 547, la quale, novellando l'art. 623 *bis* c.p., ha espressamente accomunato le comunicazioni informatiche o telematiche (che consentono trasmissioni a distanza di suoni, immagini o altri dati) alle comunicazioni di tipo telegrafico o telefonico, intercorrenti quindi tra esseri umani.
Dunque, la peculiarità delle comunicazioni di tal genere non è costituita soltanto dallo strumento di trasmissione adoperato, bensì soprattutto dalla forma digitale attraverso cui si elaborano e si organizzano i dati. Del resto, il computer, che è l'elaboratore elettronico per eccellenza, produce ed organizza i dati, per mezzo di appositi programmi (*software*[172]), appunto in forma digitale,

Commission, Digital Single Market, Digital economy & society, su https://ec.europa.eu/digital-single-market/en/digital-inclusion-better-eu-society.

172 L'insieme delle procedure e delle istruzioni eseguibili in un sistema di elaborazione dati. La specificità di un programma *software* consiste nel fatto di essere suscettibile di esecuzione automatica da parte del calcolatore.

adoperando a tal scopo il sistema binario[173] (che è il sistema di rappresentazione digitale adoperato nell'elaborazione automatica dell'informazione).

L'intercettazione informatica o telematica avrà, quindi, ad oggetto proprio i dati digitali che compongono l'informazione, elaborati, organizzati o trasmessi da un elaboratore ad un altro.

Dato questo quadro, si tenta di ricercare la definizione di "sistema informatico", al fine di meglio comprendere l'ambito attraverso cui si dipana la potenzialità dell'intrusione e captazione a mezzo di strumenti informatici, la quale, innanzitutto, è stata delineata durante la Convenzione di Budapest del Consiglio d'Europa del 2001 sulla criminalità informatica[174], laddove, invece, non essendo esplicitata alcuna nozione del sistema suddetto nella legislazione interna, si è lasciato alla giurisprudenza il compito di provvedere ad una sua delineazione.

In generale, si può considerare che gli elementi tipici siano da individuare sia in un sistema costituito da più elaboratori collegati tra di loro al fine di scambiarsi o trasmettersi dati, ma anche in ogni elaboratore elettronico, il quale si avvalga di programmi (*software*) che esprimono in determinati linguaggi (algoritmi) le specifiche operazioni da eseguire[175].

Dunque, si ritiene che anche il singolo elaboratore possa essere ricondotto nel concetto di sistema informatico, purché si intenda per tale un sistema di risorse composto da dispositivi di elaborazione elettronica digitale, programmi e gruppi di dati, che sotto il controllo di determinati programmi, immette, organizza e trasmette automaticamente dei dati che può memorizzare e recuperare[176].

A questo proposito, in un'importante pronuncia della Cassazione[177], a ciò relativa, si è voluto dare maggiore risalto al significato di "informazione" rispetto a quella di "dato", nel senso che alla

---

173 Il singolo dato digitale è denominato *bit* (*binary digit*). Per bit si intende l'unità di misura elementare dell'informazione, registrata o elaborata da un elaboratore e rappresentata alternativamente dalle cifre 0 e 1, in quanto corrisponde ad una scelta tra due alternative egualmente possibili. Una sequenza di otto bit si chiama *byte*.

174 La Convenzione del Consiglio d'Europa di Budapest sulla criminalità informatica del 23 novembre 2001, ratificata in Italia dalla l. 18 marzo 2008, n. 48, ha fornito, infatti, una definizione di base, intendendo per tale una "qualsiasi apparecchiatura isolata o un insieme di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica dei dati". Contrariamente, nella legislazione interna non si contempla alcuna definizione di sistema informatico, così costringendo l'interprete alla ricerca degli elementi caratterizzanti un sistema di questo tipo.

175 G. SARTOR, *L'informatica giuridica e le tecnologie dell'informazione*, seconda edizione, Giappichelli, Torino, 2010, 133.

176 P. GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, Giuffrè, Milano, 1997, 40.

177 Su questo tema, la Corte di Cassazione è intervenuta con un'importante decisione (Cass., sez. VI, 14 dicembre 1999, n. 214945), con la quale ha precisato che debba ritenersi sistema informatico "un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate, per mezzo di un'attività di codificazione e decodificazione, dalla registrazione o memorizzazione, per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di

funzione di registrazione e memorizzazione elettronica dei dati, intesi quali rappresentazioni elementari di un fatto, si affianca la funzione complementare di elaborazione, organizzazione e catalogazione logica di tali dati in insiemi più o meno complessi, che costituiscono appunto le informazioni.

In conclusione, si può affermare che l'elemento discretivo essenziale, al fine di individuare un sistema informatico, sia da rintracciarsi nella capacità della macchina elettronica di organizzare ed elaborare dati grazie alla lettura di specifici programmi ed eventualmente di trasmetterli ad altri elaboratori.

Per quanto concerne, specificatamente, la nozione di "sistemi telematici", si prende come punto di partenza la definizione di sistema informatico, al quale devono essere aggiunti ulteriori elementi.

Un sistema telematico si rinviene nel caso in cui la connessione tra più sistemi informatici, realizzata attraverso apparati di comunicazione (ad esempio, via modem o rete locale o *wireless*), permette la trasmissione a distanza di informazioni, precedentemente elaborate e memorizzate.

In questo caso, l'elemento che consente di ravvisare un sistema telematico in luogo di un mero dispositivo di trasmissione a distanza di segnali (come il telefono o il fax) è dato proprio dal fatto che ad essere collegati tra loro sono due o più sistemi informatici.

Anche in questo caso un contributo all'opera di definizione è stato apportato dalla giurisprudenza della Cassazione[178].

---

un fatto, effettuate attraverso simboli (bit), in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare informazioni, costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. La valutazione circa il funzionamento di apparecchiature a mezzo di tali tecnologie costituisce giudizio di fatto insindacabile in Cassazione ove sorretto da motivazione adeguata ed immune da errori logici".

178 Le Sezioni Unite della Corte di Cassazione (Cass., SS. UU., sent. 23 febbraio 2000, n. 6) hanno individuato una definizione di sistema telematico al fine di ricondurvi l'apparato di telefonia mobile. La Cassazione ha così argomentato: "In concreto, le linee telefoniche, secondo la moderna tecnologia, attuano la trasmissione delle comunicazioni con la conversione (codificazione) di segnali fonici in forma di "flusso" continuo di cifre, e detti segnali, trasportati all'altro estremo, vengono ricostruiti all'origine (decodificazione). Trattasi, dunque, di flussi relativi ad un sistema tecnico che s'innesta nella disciplina delle intercettazioni di comunicazioni informatiche o telematiche, captate a sorpresa nel corso del loro svolgimento, che hanno per oggetto anche la posta elettronica (*e-mail*) da computer a computer collegati alla rete Internet in forma ibrida per mezzo di messaggi SMS da computer, collegato a detta rete, ad apparecchi cellulari GSM o viceversa. Il flusso è il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici. Fra strumenti informatici, quindi, è possibile lo scambio di impulsi in cui si traducono le informazioni; scambio che è comunicazione al pari della conversazione telefonica, sicché la relativa captazione nel momento in cui si realizza costituisce intercettazione". La Cassazione ha voluto, con tale definizione, tentare di spiegare come i vari strumenti elettronici comunicano tra loro. Attualmente i sistemi si possono distinguere in cablati (*wired*) o *wireless*, ovvero in locali o cellulari (ove ci si appoggia ad una rete con copertura esterna variabile). Il

Viene così individuato l'intero campo potenzialmente suscettibile di essere oggetto di intrusione, ingerenze esterne o intercettazione, laddove si consideri, oltretutto, che l'intero sistema telefonico e l'intero sistema informatico siano da ricondurre, oramai, ad un gigantesco sistema telematico[179].

3. Il controllo informatico potenzialmente messo in atto da parte di chiunque. Ragioni del controllo e strumenti informatici.

La rilevanza assunta dal fenomeno del controllo informatico emerge dal suo essere attuabile da parte di un qualunque soggetto nei confronti di un altro.
Le ragioni che eventualmente muovono una persona al controllo sono rimaste le medesime del recente passato, che non offriva un panorama tecnologico così vasto e dilagante. Dato ciò, si constata il cambiamento dell'ambito all'interno del quale si dispiegano le relazioni umane, un ambito dove i dispositivi digitali e gli strumenti inforrmatici fanno imprescindibilmente parte dell'equazione sociale, che mette tutti in connessione con tutti, e dove caratteristica principale è divenuta la potenzialità insita a tali strumenti di mettere in atto agevolmente e rapidamente qualcosa di prima inattuabile con la medesima facilità, quale la realizzazione di un atto di controllo da parte di chiunque su chiunque altro.

3-a) La potenzialità di controllo insita nella tecnologia informatica.

I processi di comunicazione e gestione delle informazioni svolgono un ruolo centrale nella società contemporanea. In particolar modo, svolgono un ruolo centrale i dispositivi tecnologici che permettono questi processi e questa gestione, i quali sono sempre più essenziali nella vita quotidiana e la influenzano in modo crescente e pervasivo, condizionando, nel bene e nel male, il tempo libero e le relazioni interpersonali.
Si è compiuta così, in questi ultimi vent'anni, una trasformazione straordinaria della società e delle relazioni che in essa si dispiegano.
Sia la globalizzazione sia il passaggio ad una economia basata sui servizi appaiono strettamente correlati alla diffusione delle tecnologie digitali. Queste ultime, infatti, hanno eliminato gli ostacoli di intermediazione che si frapponevano all'accesso diretto delle informazioni e dei servizi.

---

senso che si vuole qui esprimere è che, indipendentemente dalla modalità di connessione, è possibile operare una captazione dei dati che vengono trasmessi.

179 C. PARODI, *VoIP, Skype e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?*, *Dir. penale e processo*, 2008, 1309.

É da notare che nel corso degli ultimi anni sono avvenuti cambiamenti che hanno trasformato l'organizzazione del lavoro, i processi di gestione delle attività produttive e dei servizi, le politiche del personale e anche le stesse postazioni di lavoro. Tutto ciò è stato inevitabilmente condizionato dal fatto che la tecnologia informatica (apparecchi digitali e *software*) e le telecomunicazioni (le reti telematiche) sono le basi su cui si regge la società dell'informazione. Società che ha visto mutare profondamente il concetto di comunicazione e di memorizzazione dei dati con l'avvento della c.d. rivoluzione digitale, ossia del cambiamento apportato dalla digitalizzazione degli accessi all'informazione e della registrazione degli stessi.

Si constata, inoltre, che, grazie allo sviluppo del mercato relativo, alla nuova concezione di comunicazione e alla condivisione delle informazioni apportata dalla rete, la tecnologia digitale è divenuta accessibile a tutti. Ciò sia dal punto di vista economico, poiché una tecnologia piuttosto potente, quale quella racchiusa in un *laptop* o in uno *smartphone* come quelli di uso corrente, può essere acquistata e quindi usufruita a costi notevolmente bassi rispetto al passato, ove la tecnologia dei dispositivi informatici era riservata a pochi, e sia dal punto di vista delle conoscenze circa il loro impiego. Relativamente a quest'ultimo aspetto si può certamente asserire che non occorre più essere degli esperti informatici per utilizzare questi mezzi e per trarne dal loro uso un qualsiasi tipo di vantaggio.

Alla conclusione secondo cui la tecnologia digitale sia disponibile intellettivamente a tutti, si giunge non soltanto considerando la facilità di accesso alle informazioni che permettono di capire e imparare come utilizzare uno strumento informatico, ma considerando anche che lo strumento informatico stesso è stato pensato e creato per un utilizzo che sia intuitivo, al fine di rendere possibile per ogni utente e per ogni consumatore il suo impiego, in vista del soddisfacimento nel modo più rapido possibile di una sua esigenza.

In altri termini, al giorno d'oggi, la tecnologia anche quella informatica è progettata per essere facile, per soddisfare le esigenze dell'utente medio.

L'ampia diffusione dei mezzi tecnologici e la loro disponibilità a basso costo, l'agevole reperimento delle conoscenze relative al loro utilizzo e l'intuitività d'uso che li caratterizza hanno permesso il potenziale impiego degli strumenti informatici, a fini di controllo, da parte di chiunque su chiunque, in quanto questa finalità può essere agevolmente esaudita mediante tali strumenti.

Si nota che la diffusione e lo sviluppo tecnologico, i cui benefici sono importanti ed incommensurabili, presentano anche dei risvolti minacciosi, che si insidiano nelle infinite varietà dei loro impieghi.

Non è lo strumento informatico in sé, ovviamente, ad essere pericoloso, bensì l'uso che ne viene fatto. E se, da un lato, si constata il cambiamento apportato alla vita quotidiana dai mezzi tecnologici e da Internet, essendo cambiati i modi attraverso cui comunicare, scambiarsi

informazioni ed avere ad esse accesso, dall'altro lato non si può fare a meno di constatare che la natura umana, invece, non è fondamentalmente cambiata, caratterizzandosi di atteggiamenti positivi, ma anche di comportamenti malevoli o comunque insidiosi ed invasivi.

3-b) Possibili ragioni dell'atto di controllare ed eventuali conseguenze.

La tecnologia informatica, dunque, non è altro che un mezzo che asseconda la volontà umana e ne estende ed espande l'azione ed i fini ai quali mira. Uno di questi fini può essere il controllo attuato da una persona nei confronti di un'altra.
Le relazioni umane e i loro modi di esprimersi e svilupparsi non fanno altro che avvalersi di un nuovo campo d'azione, ossia quello delle tecnologie informatiche e telematiche.
Il controllo e la volontà di dominio di un soggetto su di un altro hanno trovato una nuova e più efficace modalità attraverso cui realizzarsi.
Le ragioni che spingono la persona al controllo sono rimaste le medesime del passato, ma hanno, attualmente, la possibilità di attuarsi in un modo estremamente semplice attraverso l'impiego di poche risorse. Monitorare una persona, i suoi spostamenti, le sue comunicazioni o le sue ricerche in rete attraverso un virus-spia installato sul suo *laptop*, ad esempio, è altrettanto efficace e sicuramente più semplice e meno impegnativo che monitorarla di persona, seguendola di nascosto o cercando tra le sue cose nella sua abitazione.
Questa constatazione deriva da due considerazioni.
La prima deriva dal fatto secondo cui, al giorno d'oggi, se si vuole spiare un soggetto, il quale si avvale di dispositivi tecnologici per comunicare, cercare informazioni e salvarle, allora bisognerà ricorrere agli stessi mezzi per attuare su di lui e sui suoi dati riservati un controllo.
Come già in precedenza affermato, più ci si giova nella comunicazione, nella trasmissione di informazioni e nella loro memorizzazione delle tecnologie informatiche e telematiche, più queste attività saranno vulnerabili al controllo, effettuato attraverso strumenti che di queste tecnologie si avvalgono[180].
La seconda considerazione punta a far emergere che, ciò che distingue l'epoca contemporanea dal recente passato stia nella diversa definizione di realtà. Infatti, la realtà attuale, con cui abbiamo a che fare quotidianamente, si compone sia di esseri viventi ed oggetti fisici (realtà fisica) e sia di dispositivi artificiali e applicativi virtuali (realtà virtuale).
La realtà fisica e la realtà virtuale, a seconda dei contesti, si condizionano e si assecondano a vicenda, tanto da essere difficilmente separabili. Così, ad esempio, un controllo effettuato da un

180 Par.1, cap. 2.

soggetto su di un altro, attraverso uno strumento informatico in modo virtuale, non potrà non avere conseguenze anche nella realtà c.d. fisica di entrambi.

Si nota anche che, le azioni che intervengono nella realtà virtuale possono avvalersi di una certa disinibizione rispetto a quelle che vengono compiute fisicamente, dovuta proprio ad una mancanza di freni in quei comportamenti che nella vita reale tendono ad essere evitati, per via di limiti culturali. Disinibizione generata dalla percezione di anonimato che l'avvalersi della tecnologia informatica e della rete talvolta comporta e dalla sensazione di distanza interposta tra il servirsi dello strumento informatico e la sua conseguenza reale. Dunque, è più semplice, più pratico e presumibilmente meno coinvolgente spiare una persona attraverso una *app* apposita installata sul suo *smartphone* che, ad esempio, sottrarglielo. La partecipazione emotiva all'atto è meno forte, come se l'utilizzo stesso di un dispositivo implicasse una separazione tra l'azione compiuta, e il risultato che si vuole conseguire per il tramite di questa azione, ed il soggetto che la compie. La sensazione di separazione è rappresentata dallo schermo del dispositivo. È lo schermo, attraverso cui si interfaccia la realtà virtuale, a stabilire la distanza.

La distanza che sembra porre l'impiego della tecnologia informatica dall'atto fisico e dalle sue conseguenze, la semplicità di utilizzo dei suoi strumenti e l'esistenza stessa di questa potenzialità insita in essi possono rendere allettante l'appagamento di un desiderio di controllo.

Il controllo, nella società contemporanea, è diventato una condizione normale, qualcosa alla quale non si fa caso o su cui non ci si sofferma più di tanto[181].

Viviamo in realtà strettamente sorvegliate. Le città sono costellate da videocamere poste a difesa di edifici, banche, ospedali o installate per fotografare automobilisti o pedoni irrispettosi delle regole stradali. Dopo le rivelazioni di Edward Snowden[182], il sospetto che le comunicazioni in rete e che i cellulari fossero messi sotto controllo si è concretizzato. C'è poi l'ormai usuale realtà che vede ogni azione, compiuta usando una tastiera e un *mouse*, registrata e memorizzata da imprese che fanno del

181 O più propriamente il controllo è un concetto che può essere valutato in termini contraddittori se si va a considerare quei comuni atteggiamenti connotati dal riversare giornaliero di quantità impressionanti di dati personali su piattaforme digitali ed al contempo la preoccupazione di nascondere o criptare la propria corrispondenza o di rendere inaccessibili ad altri le proprie pagine personali che in precedenza ci si è dedicati ad arricchire di informazioni. In quest'ottica si percepisce chiara l'ambigua complicità sussistente tra la volontà di mostrarsi ed il gusto del segreto, in un quello che sembra essere un apprezzamento nevrotico di tutto ciò che è legato all'atto del controllo ed al suo oggetto. Così B. BONATO, *La possibilità della discrezione*, in AA.VV., *La trasparenza e il segreto*, Mimesis edizioni, Milano-Udine, 2017, 138 e 143.

182 Ex tecnico della CIA e fino al 10 giugno 2013 collaboratore della Booz Allen Hamilton (azienda di tecnologia informatica consulente della NSA, ossia National Security Agency), è noto per aver rivelato pubblicamente dettagli di diversi programmi di sorveglianza di massa del governo statunitense e britannico, fino ad allora tenuti segreti. G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina Editore, Milano, 2015.

commercio dei dati il loro *core business*. Infine, anche i messaggi scambiati su *Twitter* o i "mi piace" cliccati su *Facebook* diventano proprietà di queste imprese, trasformando i gusti così espressi e le interazioni così attuate in materia prima per le imprese dei big data e per gli stessi *social network*.

Le relazioni sociali, di carattere personale o lavorativo, si sono ultimamente sviluppate e continuano a svilupparsi attorno alle piattaforme dei *social network*, nelle quali il monitoraggio sulla vita virtuale, specchio (distorto) della vita reale, delle persone ad esse iscritte si svolge ed è compiuto reciprocamente. In questo monitoraggio reciproco si esprime la consapevolezza, più o meno latente, di essere controllati e soprattutto la condiscendenza ad esserlo. Il controllo, qui, è volontariamente concesso dalle parti coinvolte, le quali compiacenti ignorano le insidie che da questo tipo di atteggiamento possano scaturire.

In questo modo, controllo volontario e controllo occulto si intrecciano e perdono i loro contorni nella superficiale percezione dell'utente medio della rete o di un possessore di un dispositivo informatico.

Tutto ciò ha portato come conseguenza l'assuefazione al controllo e la superficialità diffusa nel compimento di atti ad esso finalizzati.

Dato questo contesto, si può ipotizzare che le ragioni che muovono un soggetto ad una tale azione di controllo vengano ritenute dal soggetto medesimo di per sé sufficienti a giustificarla. Infatti la trasformazione dell'azione dalla potenza all'atto è, se si vuole, facile, rapida, priva di ostacoli e la possibilità stessa della sua realizzazione induce alla tentazione di mettere in discussione quei limiti interiori posti dalla cultura e dalla società, rappresentazioni classiche dei freni indicatori di autoresponsabilità di un soggetto, nell'innesco di un meccanismo per il quale sia il mezzo a giustificare il fine[183].

Queste ragioni si ritiene scaturiscano dalla componente più primordiale della persona umana e nulla presentano di nuovo nella loro caratterizzazione. Esse fanno leva su sentimenti istintivi e su una

183 Non potrebbe essere altrimenti se si prende in considerazione la nozione di dispositivo come nozione relazionale, secondo la quale i dispositivi, che circondano ormai la nostra esistenza, non stanno di fronte all'uomo come oggetti neutri di consumo, bensì creano la personalità di chi li usa. Per G. AGAMBEN (tenendo presente le costruzioni di tale concetto in Foucault e Deleuze) il dispositivo è "qualunque cosa abbia in qualche modo la capacità di catturare, orientare, determinare, intercettare, modellare, controllare e assicurare i gesti, le condotte, le opinioni e i discorsi degli esseri viventi", capace di attivare un processo di soggettivazione e desoggettivazione. Tuttavia, quello che avviene nella fase attuale del capitalismo è che i processi di soggettivazione e desoggettivazione sembrano diventare reciprocamente indifferenti, senza dare luogo alla ricomposizione di un nuovo soggetto se non in forma larvata e spettrale. Tant'è che, ad esempio, "colui che si lascia catturare nel dispositivo telefono cellulare, qualunque sia l'intensità del desiderio che lo ha spinto, non acquista, per questo, una nuova soggettività, ma soltanto un numero attraverso cui può essere, eventualmente, controllato". In *Che cos'è un dispositivo?*, Nottetempo edizioni, Milano, 2006, 21-22, 31.

forte componente di superficialità nella valutazione delle conseguenze delle proprie azioni, nella considerazione della relazione con l'altro ed anche, presumibilmente, nella conoscenza di se stessi.
L'impossibilità a percepire che una persona, a cui si sia legati affettivamente o relazionalmente, sia un'entità separata da se stessi, un'entità altra che non sia suscettibile di dominio, può essere una delle ragioni causa di un atto di controllo. Così come può esserlo una finalità fraudolenta (frode, sottrazione di informazioni[184], ricatto) messa a punto nell'ambito lavorativo o piuttosto in generale, puntando ad una vittima qualunque (si pensi al furto della password della carta di credito attraverso un raggiro informatico, attuato, ad esempio per il tramite di un *exploit*[185]). Infine, un atto del genere può scaturire, banalmente, da semplice curiosità o noia. Sicuramente in quest'ultimo caso, come anche nel primo, l'espressione della superficialità quale componente caratterizzante nel compimento dell'azione trova il suo punto massimo. Il rischio, in questi casi, è l'innesco di comportamenti assai insidiosi e pericolosi non solo per l'altrui riservatezza, ma anche per l'individuo nella sua pienezza, in quanto suscettibili di provocare danni morali ed esistenziali. Infatti alcune di queste condotte possono scaturire in vere e proprie molestie, attualmente riconosciute e contrastate dall'ordinamento giuridico, quali quelle configuranti ciò che viene definito *cyberstalking*[186] e *cyberbullismo*[187].
Fondamentalmente, tali forme di comportamenti persecutori e violenti, attuati nell'ambito del cyberspazio, corrispondono a comportamenti aggressivi tradizionali. Gli autori di tali atti non fanno altro che utilizzare i mezzi digitali come armi nuove al fine di apportare un danno alla vittima. Danno che è diretta conseguenza dell'atto molesto in sé e non è provocato dallo strumento informatico in quanto tale. Esso costituisce solo il mezzo attraverso il quale si configura un

184 Atto compiuto anche al fine di far valere un proprio diritto in giudizio da parte del lavoratore a scapito del suo datore di lavoro. Par. 4, cap. 2.

185 Par. 3.1-a), cap. 2.

186 Il *cyberstalking* consiste nel porre in essere comportamenti persecutori nei confronti della vittima mediante l'impiego di strumenti informatici o di comunicazione elettronica. Il termine denota l'uso della tecnologia, in particolare Internet, per molestare una persona. Fra le caratteristiche comuni vi sono false accuse, monitoraggio, minacce, furto di identità e distruzione o manipolazione di dati. Le molestie possono assumere varie forme, ma il comune denominatore è dato dal fatto che sono indesiderate, spesso ossessive e solitamente illegali. La l. n.38/2009 ha introdotto in Italia il reato di stalking, definendo così quali comportamenti persecutori siano da considerarsi reato e possano essere quindi oggetto di denuncia. http://www.commissariatodips.it/approfondimenti/cyberstalking.html

187 Il *cyberbullismo* è il termine che indica un tipo di attacco continuo, ripetuto, offensivo e sistematico attuato mediante gli strumenti informatici e di connessione in rete. Alcune delle azioni che lo caratterizzano possono essere il *flaming* o l'*harassment*, consistenti nella spedizione ripetuta di messaggi *online* violenti, insultanti o volgari; l'*impersonation*, ossia il farsi passare per un'altra persona per spedire messaggi o pubblicare testi reprensibili; il *doxing*, consistente nel cercare e diffondere pubblicamente *online* informazioni private o altri dati sensibili riguardanti una persona, con intento malevolo. G. MARZANO, *Il lato maligno del Web*, Mimesis edizioni, Milano-Udine, 2016, 53-54.

compimento più insidioso per la vittima ed implicante un coinvolgimento minore del sentimento di autoresponsabilità interiore dell'autore, stante la disinibizione che il dispositivo suddetto può innescare. Disinibizione generata, come già accennato, da una distanza posta tra il soggetto e la conseguenza dell'atto che pone in essere, dovuta al dispositivo, che è mezzo di accesso alla realtà virtuale e di trasformazione della realtà fisica in realtà virtuale e viceversa. Questo schermo, in senso figurato e letterale, fomenta l'arresto di un'operazione di riconoscimento da parte di un soggetto nei confronti dell'altro soggetto quale entità a sé stante, ostacolando una presa di coscienza circa il rispetto che merita l'altro, in quanto altro individuo separato e alla pari, e precludendo un atto di autoresponsabilizzazione nei suoi confronti.
Anche qui, infine, si constata che i comportamenti minacciosi e persecutori esistono da prima dell'avvento della tecnologia informatica, poiché insiti nella natura umana, quando invece, negli ultimi anni, ad essersi modificati sono i luoghi e le modalità attraverso le quali tali atti insidiosi si esplicano.

3-c) Alcuni strumenti informatici di cui avvalersi agevolmente al fine del controllo altrui.

Per dare un'idea dell'ampia offerta di strumenti informatici volti ad un utilizzo finalizzato al controllo (occulto) altrui e del variegato assortimento di questi si possono individuare alcune tipologie esemplificative. La loro comune caratteristica, oltre alla finalità di impiego, consiste nella facilità circa il loro reperimento e la semplicità d'uso di cui si avvalgono.
Le fonti variano dalle riviste informatiche specializzate all'immediatezza della consultazione attraverso il Web, ove le modalità di impiego ed i vari passaggi relativi all'installazione e alla configurazione dello strumento informatico sono descritti in modo particolareggiato, permettendone anche ad un non esperto di servirsene.
Si può cominciare dall'illustrazione del metodo *Mac Spoofing*, volto a spiare le conversazioni effettuate attraverso *WhatsApp Messenger* o *WhatsApp Web*, noto servizio di messaggistica istantanea e di comunicazioni VoIP, usufruibile mediante la relativa applicazione (*app*) configurabile su uno *smartphone*, al fine di metterlo in contatto con un altro *smartphone*, sul quale sia installata la stessa *app*, oppure con un *personal computer*. *WhatsApp* usa la connessione Internet del telefono per mandare messaggi ed effettuare chiamate, configurando così un servizio gratuito, gravante unicamente sul traffico dati a disposizione.
Il *Mac Spoofing* indica un metodo di spionaggio che avviene grazie al *Media Access Control* (il cui acronimo è appunto Mac), ossia un codice di sicurezza composto da lettere e numeri (chiamato anche indirizzo fisico o indirizzo Ethernet/LAN), unico per ogni cellulare.

A tale scopo occorrono sia il Mac *address* dello *smartphone* in possesso di colui che vuole porre in essere il controllo e sia quello del soggetto sul quale questo controllo è rivolto[188]. A questo punto, i seguenti passaggi prevedono: la disinstallazione di *WhatsApp* da parte dell'autore del controllo dal proprio dispositivo; la sostituzione del Mac a*ddress* con quello della persona che vuole spiare (per fare ciò esistono alcune specifiche applicazioni da scaricare sul dispositivo); la re-installazione di *WhatsApp* sul suo cellulare, inserendo, quando viene richiesto, il numero di telefono dell'altra persona; la richiesta del codice di attivazione via SMS (a tal fine occorrerebbe essere momentaneamente in possesso del telefono del soggetto spiato, poiché il messaggio con il codice sarà inviato sul suo dispositivo); infine la re-impostazione del Mac *address* originale da parte del soggetto controllante sul suo cellulare. Se tutti i passaggi sono stati eseguiti correttamente, aprendo *WhatsApp* verranno automaticamente visualizzati tutti i messaggi, le foto ed i video della persona spiata[189].

Un altro esempio di monitoraggio occulto può essere quello consentito dall'utilizzo improprio dall'applicazione "Cerberus" per *smartphone* o *tablet*. Improprio perché, in realtà, tale *app* è legale ed è stata originariamente prevista allo scopo di fungere da "antifurto" per il rispettivo dispositivo. Laddove questo, infatti, venisse sottratto al proprietario, egli potrebbe prenderne il controllo da remoto, impedendone l'uso altrui. Questa *app*, tuttavia, se utilizzata con il fine specifico di spiare il

188 Questa informazione è reperibile nell'area "impostazioni" del cellulare (il che presuppone una sottrazione momentanea del telefono dell'altro soggetto), oppure, se i cellulari sono connessi alla stessa rete Wi-Fi si può trovare il Mac a*ddress* direttamente dal pc.

189 Il *Mac Spoofing* è attuabile anche per monitorare la trasmissione di dati personali compiuta da una persona attraverso *WhatsApp Web*, servizio che consente di usare l'applicazione direttamente dal pc. A tale scopo, basta impossessarsi per qualche secondo del telefono della persona che si vuole controllare, e accedere al servizio *WhatsApp Web* dal sito ufficiale inserendo il QrCode (codice composto da moduli neri disposti all'interno di uno schema di forma quadrata, che viene impiegato per memorizzare informazioni generalmente destinate a essere lette tramite uno *smartphone*). Una volta effettuato l'accesso, si rimane connessi fin quando non si effettua il *log out*. Dunque, basta riconsegnare il telefono e lasciare il pc acceso, cosicchè, da quel momento in poi, tutte le conversazioni e lo scambio dati che la vittima effettua da cellulare, verranno visualizzate sul pc del soggetto controllante. http://messaggimania.it/ultime-notizie/whatsapp-la-tecnica-per-spiare-messaggi. Dal suddetto sito, come in molti altri offrenti contenuti simili, è chiaramente sottolineato che la pratica di monitoraggio occulto dei messaggi e di altri contenuti trasmissibili per il tramite della *app* citata, messa in atto con la tecnica del *Mac Spoofing*, non è legale e declina ogni responsabilità su eventuali utilizzi illeciti delle informazioni da esso riportate. Viene sottolineato, oltretutto, che la pubblicizzazione di tali pratiche e della loro descrizione ha meri fini informativi, in modo da far prendere coscienza all'utenza sui rischi che potenzialmente si corrono, dando anche alcuni suggerimenti per difendersi da tali pratiche e per testare la sicurezza offerta dai propri dispositivi. Infine è da segnalare che, a premessa della descrizione dei passaggi componenti la tecnica di controllo e dal declino delle responsabilità sull'impiego illecito, viene messo in evidenza che tale metodo di spionaggio possa essere utilizzato da parte di chiunque, dunque anche da coloro che non hanno un'approfondita conoscenza di specifiche tecniche informatiche.

cellulare o il *tablet* di un'altra persona, può trasformarsi in un perfetto strumento di controllo, che si serve delle periferiche *hardware* dell'altrui dispositivo[190].

Infine, un sistema di spionaggio leggermente più complesso, è quello che prevede l'occultamento di un virus in una immagine (JPEG[191]), con l'intento di sottrarre dati personali presenti nel pc di un'altro soggetto o di registrare dalla webcam e dal microfono ciò che avviene intorno al dispositivo. Infatti, la vittima sarà indotta a cliccare sull'immagine, mossa da curiosità o interesse, ma questa azione permetterà ad un *file* eseguibile di andare ad insinuarsi nel sistema operativo del suo pc. In particolare, il *file* creerà un canale di comunicazione tra il pc del controllato e quello del controllante, che potrà così assumerne il pieno controllo, potendo, da remoto, vagliare e sottrarre *file* e dati personali, attivare la webcam e il microfono per registrare video e audio ed anche installare un *keylogger*[192] per il cui tramite è possibile, ad esempio, scoprire delle password che vengano digitate sulla tastiera[193].

---

190 Al fine di compiere un'azione di controllo, l'installazione della suddetta *app* e il suo occultamento su un dispositivo altrui, è seguito dall'accesso, dal pc del controllante attraverso il sito (cerberusapp.com), all'*account* corrispondente, attuando così il controllo remoto dell'applicazione. A questo punto, è possibile avere il controllo della fotocamera e del microfono dello *smartphone* o *tablet* del controllato, il quale basta che sia connesso alla rete Internet, e scattare foto o registrare video che saranno visualizzabili in allegato ad una *e-mail* ricevuta alla casella di posta elettronica precedentemente indicata quale requisito di creazione dell'*account* della *app*. Da Speciali Win Magazine, n. 27, *Il manuale dell'hacker 2017*, Edizioni Master, Novembre/Dicembre 2016.

191 Acronimo di Joint Photographic Experts Group, è un comitato ISO (la più importante organizzazione a livello mondiale per la definizione di standard o norme tecniche)/CCITT (ora ITU-T, acronimo di International Telecommunication Union-Telecommunication Standardization Bureau, ovvero rappresenta il settore dell'Unione internazionale delle telecomunicazioni che si occupa di regolare le telecomunicazioni telefoniche e telegrafiche), che ha definito il primo standard internazionale di compressione dell'immagine digitale a tono continuo. JPEG indica quindi anche il diffusissimo formato di compressione a perdita di informazioni ed è un formato aperto e ad implementazione gratuita. Attualmente JPEG è lo standard di compressione delle immagini fotografiche più utilizzato.

192 Il *keylogger* è uno strumento *hardware* o *software* in grado di effettuare lo *sniffing* della tastiera di un computer, cioè è in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente si accorga di essere monitorato. Nel caso si tratti di un *software*, questo è creato appositamente per rilevare e memorizzare la sequenza dei pulsanti che viene digitata sulla tastiera del computer monitorato.

193 In breve, ciò è consentito grazie all'utilizzo, ad esempio, di Kali Linux, ossia un sistema operativo (particolare distribuzione di Linux) già corredato di tutti i *tool*, in realtà, necessari a testare la sicurezza dei dispositivi (attraverso il *penetration testing* ed il *security auditing*, come descritto suhttp://it.docs.kali.org/introduction-it/che-cosa-e-kali-linux.). Mediante uno dei *tool* previsto nella distribuzione Kali Linux (SET, acronimo di *Social Engineering Tools*) è possibile predisporre un canale di comunicazione nascosto tra i due pc e trasferire il *payload* del virus (ossia ciò che configura l'insieme di operazioni che un virus esegue all'interno della macchina) e l'immagine prescelta su un Web server, con lo scopo di rendere accessibile il suo contenuto anche ad altri pc, attraverso la rete. Infine il virus, che attraverso una conversione operata con un altro *tool* viene fatto somigliare all'anteprima di una fotografia digitale, verrà inviato tramite *e-mail* alla vittima, la quale potrà così essere tratta in inganno e cliccare sull'immagine. Sempre da Kali Linux,

3.1 Breve indagine sulle altre recenti ragioni del controllo informatico. Il fenomeno Anonymous e l'attivismo digitale.

Il controllo porta con sé la necessità che venga effettuato in modo anonimo, affinché i risultati che si intendono ottenere o le informazioni che si vogliono sottrarre non siano condizionati dalla consapevolezza del controllo operato e anche affinché colui che lo attua non venga scoperto e sottoposto alle conseguenze giuridiche del caso, essendo che la messa in atto di un'azione di monitoraggio informatico e di eventuale violazione dei sistemi, se condotta da un privato nei confronti di un altro privato, configura un atto illecito.

Detto ciò, è da considerare che, al giorno d'oggi, con le tecnologie che sono a disposizione e per i motivi più eterogenei, chiunque può attuare una forma di controllo informatico in modo anonimo.

Il metodo per non lasciare tracce del passaggio informatico in un computer o in un sistema altrui è ampiamente e dettagliatamente descritto in plurime fonti, rese, dalla diffusione di Internet e dalla grande offerta tecnologica, a disposizione di tutti coloro che si vogliano applicare nell'apprendimento delle tecniche relative.

Basta una conoscenza informatica poco più che di base per seguire, "passo passo", la descrizione delle operazioni da eseguire nell'intento di agire anonimamente[194].

L'anonimato è una condizione che può essere raggiunta grazie all'utilizzo, ad esempio, del protocollo *Tor* (acronimo di *The Onion Router*), che configura un sistema di comunicazione anonima per Internet. Scopo di questo *software* è quello di proteggere gli utenti dall'analisi operata sul traffico attraverso una rete di *router* (detti *onion router*), gestiti da volontari, che permettono il traffico anonimo in uscita e la realizzazione di servizi anonimi nascosti.

Tramite il suo utilizzo è molto più difficile tracciare l'attività Internet dell'utente, difatti l'uso di questo *software* è finalizzato a proteggere la privacy degli utenti, la loro libertà e la possibilità di condurre delle comunicazioni confidenziali senza che vengano monitorate[195].

---

con uno specifico comando (*msfconsole*, che attiva il *software* "Metasploit"), avvia il *payload* creato in precedenza, che in caso di immagine cliccata da parte della vittima, consentirà il controllo del suo computer. Speciali Win Magazine, n.27, *Il manuale dell'hacker 2017*, Edizioni Master, Novembre/Dicembre 2016.

194 Uno di questi *vademecum* di facile reperibilità è il "Manuale pratico dell'apprendista Anonymous" (su www.winmagazine.it/link/3334.), messo a disposizione non solo di coloro che vogliano agire con modalità anonima sul Web, ma anche di coloro che vogliano farlo, ad esempio, in aderenza agli scopi prefissatisi dagli attivisti di Anonymous.

195 Per quanto riguarda il funzionamento di Tor, questo prevede che i dati , appartenenti ad una qualsiasi comunicazione, non transitino direttamente dal *client* al *server*, ossia in maniera diretta attraverso Internet dal mittente al suo destinatario, bensì passino attraverso i *server* Tor, i quali agendo da *router*, costruiscono un circuito virtuale crittografato a più livelli (in analogia all'*onion*, cioè in italiano "cipolla"), suddividendo i dati che compongono la

In questo modo ci si potrà avvalere in maniera anonima dei servizi di comunicazione messi a disposizione da Internet (ad esempio, pubblicando *online* informazioni od articoli), senza il timore di incorrere in un eventuale controllo finalizzato a risalire all'indirizzo IP reale dell'operatore con il rischio di identificarlo [196].

3.1-a) Il fenomeno Anonymous quale esempio di intento di monitoraggio.

La facile reperibilità di questi strumenti informatici se unita ad uno specifico scopo (o, meglio, ad uno specifico ideale), ossia il realizzare servizi digitali al fine di garantire, all'utente e a se stessi, libertà di espressione e ricerca di trasparenza delle dinamiche messe in atto dai poteri forti, quali l'autorità statale e l'autorità economica, rappresentata dalle multinazionali, va a generare quella che può essere definita un'adesione agli ideali del fenomeno Internet di Anonymous.
Sono anni che si sente parlare di Anonymous. Tuttavia, c'è ancora molta confusione su cosa sia davvero questo fenomeno, a causa della difficoltà che si incontra nel definire con esattezza la tipologia di azioni compiute da chi sostiene di agire come Anonymous.
Comunemente, le azioni da questi operate vengono fatte rientrare nella definizione di *hacktivism*, termine che, nato dall'unione delle parole *hacking* e *activism*, vuole indicare un modo di agire volto alla difesa della libertà di espressione e dei diritti civili, attraverso l'impiego di strumenti informatici e pratiche digitali.
Le attività di chi si riconosce nell'azione collettiva generata o ispirata ad Anonymous, possono riguardare sia la messa in atto di forme di protesta effettuate *online*, come il *netstrike*[197], sia la

---

comunicazione in diverse parti singolarmente intelligibili ed instradandole, attraverso differenti percorsi sulla rete, fino al destinatario finale. Tale operazione ha lo scopo di rendere difficilmente rintracciabile dai fornitori dei servizi di connessione ad Internet (*provider*) sia il contenuto della comunicazione che il mittente ed il destinatario. Analogamente è possibile utilizzare Tor attraverso degli appositi *browser* (con ciò si fa riferimento ad un programma che consente di visualizzare i contenuti delle pagine dei siti Web e di interagire con essi, permettendo così all'utente di navigare in Internet, grazie all'interpretazione e alla visualizzazione dell'HTML, *HyperText Markup Language*, cioè il linguaggio con il quale sono scritte la maggior parte delle pagine Web. Un esempio è *TorBrowser*) al fine di garantire all'utente l'anonimato per quanto concerne le pagine Internet visitate. Su https://svn.torproject.org/svn/projects/design-paper/tor-design.html.

196 Queste operazioni rivestono una particolare imporatnza, ad esempio, per determinati soggetti, quali giornalisti o semplici cittadini di Paesi dove la libertà di stampa e i diritti civili in generale siano limitati, i quali hanno la possibilità, attraverso tali strumenti, di pubblicare notizie sui crimini di governo o sulla situazione politica corrente, senza il rischio di dover essere censurato o arrestato. Si pensi alla situazione politica durante la rivoluzione in Ucraina (e corrente) o in Turchia con l'attuale presidenza di Erdogan.

197 Il *netstrike* può essere definito come un attacco informatico non invasivo, in quanto non va a penetrare o modificare programmi o sistemi informatici, che consiste nel moltiplicare le connessioni contemporanee al sito preso di mira, al

pubblicazione di informazioni riservate, acquisite tramite incursioni informatiche compiute per il tramite di *exploit*[198], *phishing*[199] e metodi di ingegneria sociale[200], sia la modifica o il blocco temporaneo delle attività *online* del target, ottenibili attraverso tecniche di *defacement*[201] e DDoS[202] [203].

---

fine di rallentarne o impedirne le attività. Questo attacco avviene ripetendo in maniera coatta il *refresh* della pagina in questione, provocando così la saturazione delle risorse della macchina che ospita il sito e, di conseguenza, rendendolo inaccessibile.

198 Un *exploit* costituisce lo sfruttamento di una specifica vulnerabilità presente in un sistema informatico, in modo da permettere l'esecuzione di un codice estraneo su di esso con lo scopo di far ottenere, a colui che effettua l'attacco, il controllo del computer, avvalendosi di una certa tipologia di *script* (che può essere visto come un insieme di strumenti "preconfezionati" per la programmazione, più facili da utilizzare rispetto ai tradizionali linguaggi. Esso designa un tipo particolare di programma, scritto in una particolare classe di linguaggi di programmazione, detti linguaggi di *scripting*), virus o *worm* (che indica una particolare categoria di *malware* in grado di autoreplicarsi. È simile ad un virus ma, a differenza di questo, non necessita di legarsi ad altri eseguibili per diffondersi, ma si diffonde spedendosi direttamente agli altri computer, ad esempio, tramite *email* o una rete di computer. Tipicamente un *worm* modifica il computer che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e rimanere attivo finché non si spegne il computer o non si arresta il processo corrispondente. La replicazione solitamente avviene sfruttando la rete Internet). È possibile che un *exploit* lavori in due fasi, ovvero prima acquisisca un accesso con i minimi privilegi e solo successivamente questi vengono elevati fino ad arrivare a *root* o *administrator*. Ciò permette di prendere il pieno controllo della macchina in modo incrementale e deflazionato nel tempo, abbassando così il sospetto di attacco informatico. https://blog.kaspersky.it/exploits-problem-explanation/6393/.

199 Il *phishing* indica una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Si può concretizzare attraverso messaggi di posta elettronica ingannevoli, come ad esempio, una *e-mail*, solo apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l'accesso previa registrazione (web-mail, e-commerce ecc.). Il messaggio invita a fornire i propri riservati dati di accesso al servizio ed indica, solitamente, un collegamento (link) che rimanda solo apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrati.In realtà il sito a cui ci si collega è stato allestito con fattezze identiche a quello originale, in modo da trarre in inganno la vittima ed indurla così ad inserire i suoi dati riservati, i quali verranno trasmessi all'autore della truffa. https://www.commissariatodips.it/approfondimenti/phishing.html

200 Nel campo della sicurezza informatica, l'ingegneria sociale (*social engineering*) è lo studio del comportamento individuale di un soggetto al fine di carpirne informazioni, mettere in atto frodi o accedere a sistemi privati, mediante tecniche psicologiche ed informatiche di inganno. É una tecnica riconducibile al *phishing* generalmente impiegata laddove la rete oggetto dell'attacco non presenti un *bug* (errore nella struttura del programma), che avrebbe potuto essere sfruttato a fini di hackeraggio, e quindi si vanno a ricercare i punti deboli del c.d. fattore umano, tentando di estorcere direttamente dalla persona informazioni utili. Viene utilizzata soprattutto in casi di spionaggio industriale a livello internazionale. *Minacce: come evitare gli attacchi di phishing e Social Engineering*, https://www.certnazionale.it/documenti/2015/03/02/minacce-come-evitare-gli-attacchi-phishing-social-engineering/

201 Con *defacement* o *defacing* (in italiano letteralmente "defacciamento") si vuole indicare la modifica della *home page* di un sito Web oppure la modifica o sostituzione di più pagine interne. Generalmente, le tecniche utilizzate per

Il fenomeno Anonymous non identifica un gruppo con struttura gerarchica o organizzata in tal senso, poiché non esistono capi né esistono veri e propri membri. Anonymous è piuttosto un modo di comportarsi, un modo di fare politica su Internet, all'insegna della manifestazione e difesa di determinati ideali. Ciò avvalendosi di azioni di "pirateria informatica" con l'intento, ad esempio, di porre sotto la gogna mediatica determinate persone che hanno agito in un modo ritenuto ingiusto o di svelare segreti di enti governativi o multinazionali, al fine di palesare e diffondere, attraverso i mezzi della tecnologia, un ideale di etica personale, politica e professionale[204].

Grazie agli strumenti della pirateria informatica, diventa possibile entrare nei computer o nelle risorse *cloud* dei soggetti presi di mira, trovare prove della loro colpevolezza e svelare pubblicamente l'identità e le azioni criminali da questi commesse, sui siti Web o sui *social network*, affinché poi la giustizia possa fare il suo corso.

Oltre ai tradizionali soggetti monitorati dagli attivisti di Anonymous, si è aggiunta di recente una nuova categoria, ossia quella dei terroristi, in particolare gli estremisti appartenenti all'autoproclamato Stato Islamico.

Alcuni pirati di Anonymous operano con lo scopo di intercettare i loro piani terroristici o di impedire la divulgazione, attuata attraverso il Web, dei video o dei comunicati da questi creati a fini propagandistici per la ricerca di nuovi militanti o rintracciando e sottraendo il denaro a disposizione dell'organizzazione terroristica. Ad esempio, queste operazioni vengono adempiute oscurando o

---

ottenere i permessi di accesso in scrittura al sito sfruttano solitamente i *bug* presenti nel *software* di gestione del sito oppure nei sistemi operativi sottostanti.

202 Il DDoS è una variante dell'approccio DoS (acronimo di *Denial of Service*), ove quest'ultimo si riferisca ad un attacco informatico in cui si fanno esaurire deliberatamente le risorse di un sistema informatico, che fornisce un servizio ai *client*, provocandone un malfunzionamento. Un attacco DoS è un attacco mirato ad arrestare un computer o una rete, per impedirne l'accesso da parte degli utenti effettivamente autorizzati, che si compie inondando l'obiettivo con traffico di dati o inviando informazioni che generano un blocco. Un attacco DDoS (*Distributed Denial of Service*) è una variante di un attacco DoS che impiega un vastissimo numero di computer infetti per sovraccaricare il bersaglio con traffico fasullo. Per raggiungere le dimensioni necessarie, gli attacchi DDoS vengono spesso eseguiti da *botnet* in grado di aggregare milioni di computer infetti affinché partecipino involontariamente all'attacco, al fine di inondare l'obiettivo remoto con traffico di dati e quindi di causare un blocco. La distribuzione molto ampia dei sistemi infetti (spesso in tutto il mondo) rende estremamente difficoltoso individuare la posizione in cui si trova l'autore effettivo dei suddetti attacchi. S. MC CLURE, J.SCAMBRAY, G.KURTZ, *Hacker! 7.0 Nuove tecniche di protezione*, Apogeo Editore, Milano, 2013.

203 Elenco delle attività che non vuole essere esaustivo bensì esemplificativo.

204 Per esemplificare la finalità delle azioni, coloro che si sentono appartenenti al movimento Anonymous, generalmente, prendono di mira criminali internazionali, pedofili, politici e burocrati corrotti o multinazionali che svolgono attività considerate scorrette. L'obiettivo è intervenire, con azioni pur sempre illecite dal punto di vista giuridico, ma ritenute corrette sul piano etico, per punire in quegli ambiti dove la giustizia si ritrova impotente.

bloccando i siti attraverso i quali questi filmati sono diffusi (mediante un'azione di *defacement*), interrompendo le loro comunicazioni o ancora svelando l'identità dei militanti.

È stato subito dopo gli attacchi di Parigi del 13 novembre 2015 che Anonymous ha lanciato un'operazione globale contro la presenza *online* dell'Isis, esponendosi, nuovamente, quale avamposto nella lotta al terrorismo[205]. Sono stati così individuati centinaia di profili *Twitter* e *Facebook* e siti Web di presunti jihadisti o simpatizzanti, i quali sono stati colpiti con attacchi informatici finalizzati sia all'oscuramento e sia, soprattutto, alla ricerca di informazioni da sottrarre.

Si inizia lavorando sulle fonti aperte e sui motori di ricerca al fine di trovare gli *account* sospetti. Alcuni di questi compiti sono automatizzati mediante l'impiego di programmi appositi, *script* e *bot* che agevolano la procedura di segnalazione del profilo *social*[206].

L'obiettivo della lotta al terrorismo ha fatto nascere numerose organizzazioni di *hacker* ed esperti di cybersicurezza, che condividono la filosofia di Anonymous (si fanno gli esempi di GhostsecurityGroup e Ghostsec.org), le quali hanno iniziato a collaborare addirittura con l'*intelligence* governativa. Fatto eccezionale se si pensa al normale contrasto operato dal potere statale alle azioni illecite (poiché le azioni di pirateria informatica messe in atto da privati, qualunque sia lo scopo, sono pur sempre azioni illecite) e all'ulteriore contrasto ad azioni di *hacking* che spesso, e in un passato recente, hanno avuto ad oggetto proprio opere di svelamento di segreti statali e governativi (Si pensi alle campagne ambientaliste o di denuncia governativa contrastate dalle agenzie di sicurezza governative, lanciate a partire dagli Stati Uniti).

Senza contare che gli stessi governi, proprio in nome della lotta al terrorismo, stanno varando leggi rigidissime in materia di controllo della rete, tema su cui gli *hacker* di Anonymous o di organizzazioni ad esso ispirate si sono sempre battuti in difesa del diritto di operare liberamente sulla rete.

Dunque, due facce della stessa medaglia del controllo (autorità pubblica e *hacker*), con interessi e obiettivi sostanzialmente contrapposti, si trovano, in questo momento storico, alla luce delle recenti vicende, ad operare insieme verso il comune obiettivo del monitoraggio e del contrasto al terrorismo. Che poi le finalità di questa lotta e le giustificazioni del controllo a tal fine dispiegato

---

205 Si ricorda l'impegno del movimento profuso nelle campagne lanciate sul Web in seguito all'attentato alla sede del giornale Charlie Hebdo del 7 gennaio 2015.

206 Le segnalazioni dei profili sospetti provengono dagli utenti e da coloro che intervengono nell'operazione. Gli utenti, che partecipano alla chat pubblica di Anonymous, segnalano gli *account* equivoci, inserendo il relativo collegamento nel *pad* (foglio *online*). Ogni tot ore, le segnalazioni raccolte sui vari *pad* vengono controllate e aggiunte alla lista dei target da inserire nei *software*. Infatti, ai fini di una prima scrematura, vengono utilizzati programmi che setacciano, ad esempio, i *tweet* o le parole utilizzate nei *post* su *Facebook*, sulla base di parole chiave come gli *hashtag*, oppure adoperano un sistema di "ricerca per immagini". Da articolo di C. FREDIANI del 16 novembre 2015, *Anonymous contro Isis: come funziona la campagna degli hacktivisti nata dopo Parigi*, La Stampa.

presentino sfumature differenti è un dato di fatto, che si individua nella constatazione che l'interesse dello Stato è rivolto ad assicurare l'ordine pubblico, mentre per l'attivista informatico il fine ultimo è il raggiungimento di un ideale etico e di giustizia che, in molte parti del mondo e anche in Occidente, in diverse situazioni, l'autorità statale non è in grado di garantire.

3.1-b) L'attivismo digitale e il rinnovato significato dell'*hacking*.

Nel quadro descritto, gli attivisti digitali riescono a porsi quale baluardo della libertà di espressione e di difesa dei diritti civili in generale, agendo per opporsi a forme di governo liberticide e a politiche votate al controllo dei comportamenti dei cittadini.
Grazie a dispositivi tecnologici, di uso ormai comune (pc portatili, *smatphone*, *tablet*) e ad una funzionale conoscenza dei dispositivi informatici e delle reti telematiche, compiono un'opera di denucia ed informazione, eliminando i filtri che i poteri della società odierna hanno interposto tra la verità e la conoscenza collettiva, e facendo risaltare la necessità di un mondo più trasparente e l'urgenza della tutela dei diritti dell'individuo, ancora violati.
Sono coloro che si oppongono ad uno status quo fatto di omertà, silenzi e violenze e reagiscono a tutto questo attraverso i mezzi dell'informazione e dell'informatica, in una lotta per la libertà che fa di loro i nuovi rivoluzionari. La tecnologia ha reso la rete la nuova piazza dove manifestare, fenomeno questo che, precedentemente all'esponenziale sviluppo ed espansione tecnologica degli ultimi anni, non aveva e non poteva avere questa eco.
Queste persone, tendenzialmente, lavorano nell'ombra, non compiono gesta clamorose e non si autodefiniscono *hacker*, volendo quasi accentuare il carattere prettamente funzionale delle loro competenze informatiche agli scopi che si prefiggono.
Spesso le loro battaglie sono condotte in silenzio, con piccoli gesti che, nel loro insieme, assumono un'impatto enorme, poiché in tal modo, riescono a costruire tanti tasselli di un mosaico, che lentamente prende forma, andando a rappresentare quell'avamposto di valori etici che, assai di frequente, viene scalfito nel tempo contemporaneo[207].
Le idee scaturite al fine di cambiare le cose sono semplici e di grande efficacia e, a tal proposito, si può nominare, quale caso esemplificativo, la vicenda di David Kobia, un giovane informatico keniota, che ha creato e sviluppato il progetto *open source Ushahidi* (che in Swahili significa "testimone"),premiato nel 2010 dalla rivista Technology Review[208].

207 G. ZICCARDI, *Hacker: il richiamo della libertà*, Marsilio, Venezia, 2011.

208 Celebre rivista del MIT che premia quei giovani informatici che stanno cambiando il mondo delle tecnologie, al fine anche di apportare miglioramenti alla condizione umana.

Il suo progetto raccoglie segnalazioni, testimonianze, diari e report di comuni cittadini e le rappresenta su una mappa interattiva, affinché frodi e brogli elettorali o episodi di violenza etnica ed, in generale, situazioni degne di essere monitorate per la loro gravità possano essere più facilmente denunciate, evidenziate anche visivamente e rese conoscibili globalmente. Il *software* si basa sull'idea di *eyewitness*, cioè di testimonianza visiva di quanto sta accadendo in parti del mondo colpite da situazioni critiche. Le testimonianze vengono rivelate su una mappa, baipassando le tradizionali fonti di informazione che spesso non sono accessibili o forniscono volontariamente notizie distorte, errate o incomplete[209].

Attraverso il suo programma si mette in atto un controllo operato da chiunque sia interessato a monitorare una situazione in un determinato territorio, colpito o interessato da un determinato evento che si vuole testimoniare, e ciò è concesso e garantito dal fatto che moltissime persone sono, al giorno d'oggi, in possesso di dispositivi tecnologici, che sono capaci di mettere in atto un controllo anche visivo immediato e che sono, al tempo stesso, in grado di diffondere e condividere in modo rapidissimo l'informazione carpita, attraverso la rete Internet.

In questa prospettiva essere *hacker* ha un nuovo senso, che si è plasmato inevitabilmente, sulle vicende politiche e umane del nostro tempo, nell'urgenza di far emergere valori che continuano ad essere elusi e di difendere diritti che continuano ad essere calpestati, laddove la tecnologia diventa strumento e campo di battaglia per questa lotta digitale.

Si vuole, però, ricordare che, in questa prospettiva della lotta in vista di un ideale mediante i mezzi della tecnologia e dell'informatica , si pone anche chi perpetra l'obiettivo di diffondere ed imporre una ideologia alla cui base vi è l'elusione completa e deliberata di ogni diritto civile, in una mortificazione dell'essere umano e del vivere sociale.

Si fa riferimento, come già in precedenza rilevato, all'organizzazione dello Stato Islamico e di coloro che vi militano e che pongono, a tal scopo, in essere anche azioni che sfruttano la risorsa

209 L'occasione della nascita di questo *software* è stata quando, nel 2007, si verificarono gravi disordini in Kenya, a seguito delle elezioni presidenziali. Il presidente aveva imposto un *blackout* mediatico in tutta la nazione e solo la rete Internet era rimasta quale canale aperto di comunicazione. Così Kobia, che era espatriato e viveva a Birmingham, ideò un sistema per fare il *tracking* (tracciamento visuale) su una mappa di ciò che stava capitando nel suo Paese d'origine. Da qui, l'ideazione di un applicazione per dispositivi che può essere utilizzata al fine di tenere sotto controllo una situazione di un determinato luogo in un determinato tempo e ricevere informazioni a riguardo. Il progetto è basato su standard aperti, quindi ad ogni nuova installazione il sistema si evolve, perché la rete di "testimoni" aumenta, aggrega e collega mappe, report e fatti appartenenti a molteplici contesti diversi. Tutte le segnalazioni sono vagliate e confrontate con altre fonti, poi convalidate e collocate sulla mappa, in tempo reale o nell'arco di pochissimo tempo. *Ushahidi* si è dimostrato efficace durante le elezioni in Sudan, per documentare le violenze a Gaza e anche per assistere i soccorritori dopo il terremoto ad Haiti. Da articolo della redazione del MIT Technology Review, *Innovators under 35*, 2010, su www2.technologyreview.com/tr35/profile.aspx?TRID=947

informatica e telematica, grazie alla disponibilità e alla facile acquisizione dei mezzi e della conoscenza tecnologica. Qui l'*hacking* è messo al servizio di un'altra ideologia, che si costruisce e si rafforza attraverso opere divulgative, al fine di reclutamento di nuovi affiliati, o la creazione di reti di comunicazione tra militanti in tutto il mondo, al fine dell'organizzazione e del compimento di atti terroristici.

Dunque, si nota, che l'*hacking*, le conoscenze informatiche e il mezzo tecnologico in genere sono solo degli strumenti funzionali ad uno scopo, che grazie o a causa della diffusione e della facile reperibilità ed accessibilità della tecnologia e del *know how* ad essa annesso può avere un riverbero sulle vicende personali e sociali ampissimo.

In conclusione, al giorno d'oggi, la grande disponibilità tecnologica, l'affidamento fatto sulla condivisione in rete e la ricerca di soluzioni semplici, efficaci e creative sono elementi posti alla base della connotazione dell'attivista digitale e della rinnovata caratterizzazione dell'attività di *hacking*, tenendo presente che una sua componente è costituita anche e soprattutto dal suo essere contemporaneo, intendendo per tale "colui che riceve in pieno viso il fascio di tenebra che proviene dal suo tempo"[210], dal suo essere consapevole di ciò e dalla sua volontà di cambiare le cose.

4. Il possibile controllo del lavoratore sul datore di lavoro.

In questa sede si vuole provare ad analizzare l'ipotesi in cui sia il prestatore di lavoro ad operare una qualche forma di controllo, soprattutto per il tramite di strumenti informatici e telematici, sul suo datore di lavoro.

A ciò fanno da premessa le considerazioni svolte in precedenza circa il fatto che la tecnologia informatica mostra, per una serie di caratteri ad essa collegati quali la facile accessibilità e la disponibilità, la sua attitudine ad essere adoperata per svolgere atti di carpimento di informazioni riservate e, quindi di controllo, e, allo stesso tempo, essendo essa ormai il mezzo principale di memorizzazione e catalogazione di informazioni di qualsiasi genere, mostra anche la sua vulnerabilità a tali atti di controllo. Atti di controllo che, si ribadisce, possono essere realizzati da chiunque e, dunque, anche da un lavoratore sul datore di lavoro.

In questo caso gli interessi in gioco sono quelli appartenenti alle due parti del rapporto lavorativo, e di conseguenza si assume che le ragioni del controllo possano risiedere proprio nelle dinamiche che all'interno di esso si dispiegano.

Si è analizzato nel primo capitolo come l'interesse del datore di lavoro a controllare l'esatta esecuzione della prestazione dovutagli sia tutelato e giustificato alla luce del più generale potere direttivo attinente alla sua posizione nella relazione lavorativa, espressamente previsto dagli artt.

210 G. AGAMBEN, *Che cos'è il contemporaneo?*, Nottetempo edizioni, Milano, 2008.

2104, 2105 e 2106 c.c. Infatti, nell'ambito del rapporto lavorativo, il potere di controllo è ritenuto connaturato alla posizione contrattuale del datore di lavoro, giacché da solo il potere direttivo non potrebbe garantire la piena e sicura realizzazione dell'interesse a ricevere la prestazione prevista contrattualmente.

Inoltre si è visto come una specifica forma di controllo datoriale sia quella prevista dall'art. 4 Stat. Lav., come riformato dall'art. 23 del d.lgs. 151/2015, inerente alla disciplina dell'impiego ed installazione degli impianti audiovisivi e degli altri strumenti dai quali derivi la possibilità di un atto di controllo, compresi gli strumenti di lavoro e gli strumenti di registrazione degli accessi e delle presenze. La peculiarità sta nel fatto che si realizzi, in questi casi, un controllo definito "a distanza", il cui concetto fa riferimento sia alla distanza fisica che temporale, determinando così la ininfluenza, nell'applicazione della disciplina inerente, di fenomeni quali il mancato funzionamento delle apparecchiature, la consapevolezza della loro presenza da parte dei lavoratori oppure l'utilizzo discontinuo delle stesse ai fini di controllo[211]. La distanza è anche ciò che fa sì che il controllo possa realizzarsi in maniera insidiosa, talvolta occulta, a maggior ragione se si avvale di strumenti informatici e telematici. É stata proprio la diffusione e pervasione della tecnologia e dell'informatica nella vita lavorativa a richiedere la modifica dell'art. 4, il quale non poteva più prescindere da un aggiornamento reso necessario dall'esigenza di porre la norma al passo con i tempi. Tutto ciò in considerazione del fatto che il controllo operato dal datore di lavoro trovi comunque la sua limitazione nell'esigenza del lavoratore di vedersi riconosciuta la tutela alla dignità ed alla riservatezza, innescando quella delicata ricerca di bilanciamento tra le contrapposte esigenze delle parti.

Dalla disciplina contenuta sia nel Codice civile che nello Statuto dei lavoratori si desume come il controllo messo in atto dal datore di lavoro sia legittimo ed espressamente previsto, poiché confacente al ruolo da lui svolto nella relazione lavorativa, pur sempre nel rispetto della persona del lavoratore e dei suoi diritti.

La situazione in cui si realizzi l'inversione delle parti nell'atto di controllare l'attività e le informazioni altrui non trova una conferma in termini di legittimazione normativa, la quale non giustifica l'interesse del lavoratore ad un eventuale controllo sul datore di lavoro. Interesse che si ritiene non giustificabile sia alla luce degli artt. 2104 e 2105 c.c, che prescrivono l'obbligo di

211 In questo senso si è espressa la giurisprudenza della Cassazione: "Il divieto posto dall'art. 4 stat. Lav. al datore, di far uso di impianti audiovisivi e di altre apparecchiature per fini di controllo a distanza dell'attività dei lavoratori, non è escluso né dalla circostanza che tali apparecchiature siano state solo installate ma non siano ancora funzionanti, né dall'eventuale preavviso dato ai lavoratori, i quali quindi sono avvertiti del controllo suddetto, né infine dal fatto che tale controllo sia destinato ad essere discontinuo, perché esercitato in locali dove i lavoratori possono trovarsi solo saltuariamente". Cass., sez. lav., 6 marzo 1986, n. 1490.

diligenza e di fedeltà a cui è tenuto il prestatore di lavoro e sia degli artt. 1175 e 1375 c.c, che prescrivono i doveri di correttezza e buona fede nell'adempimento del contratto e che incidono anche sulla posizione debitoria del prestatore. Infatti, in questo caso potrebbe ben configurarsi una violazione anche di tali doveri, laddove si assuma che i precetti ex artt. 1175 e 1375 abbiano un ruolo nell'esecuzione del contratto di lavoro, ed in particolare nella conformazione degli obblighi del lavoratore[212]. Questa considerazione andrebbe ad introdurre nel rapporto di lavoro una serie di obblighi accessori, autonomi rispetto all'adempimento della prestazione principale, ma comunque derivanti dall'assunzione del vincolo negoziale, che non solo accompagnano l'unidirezionale obbligo alla collaborazione all'interno dell'impresa da parte del lavoratore (come previsto dall'art. 2094 c.c.[213]), ma anche indirizzano ciascuna delle parti a preservare l'utilità l'una dell'altra, mediante linee di comportamento finalizzate a garantire la collaborazione e la lealtà reciproca in vista della realizzazione del contratto[214].

Si può fare un breve inciso in merito al fatto che, in passato, la clausola in particolare di buona fede fosse stata impiegata soprattutto al fine di un'interpretazione volta al contenimento dei poteri datoriali, in funzione correttiva dell'originario squilibrio tra le posizioni soggettive delle parti nel rapporto di lavoro, ove una è subordinata all'altra[215]. Tuttavia, nonostante questa originaria resistenza all'ampliamento degli obblighi del lavoratore, si pone come opportuna una considerazione dei precetti di correttezza e buona fede finalizzata all'individuazione di quei doveri di cooperazione del lavoratore che, non aventi quale oggetto *stricto sensu* l'adempimento della prestazione dedotta nel contratto, sono in ogni caso volti alla salvaguardia della collaborazione

212 La dottrina e la giurisprudenza giuslavoristiche hanno ricondotto la correttezza e la buona fede alla categoria delle clausole generali, aventi funzione integrativa del contratto idonea ad arricchire il contenuto del rapporto obbligatorio di lavoro. Tra i molti, A. PERULLI, *Il controllo giudiziale dei poteri dell'imprenditore tra evoluzione legislativa e diritto vivente*, *Riv. it. Dir. Lav*., I, 2015, 90 ss.; P. GALLO, *Contratto e buona fede. Buona fede in senso oggettivo e trasformazioni del contratto*, Utet, Torino, 2014, 614 ss.

213 "L'obbligo di collaborazione del lavoratore soddisfa l'interesse del datore di lavoro al coordinamento e quindi all'organizzazione dell'attività lavorativa del lavoratore stesso. Esso pertanto non si risolve soltanto nello svolgimento delle mansioni pattuite, ma nello svolgimento di tali mansioni in vista del risultato perseguito dall'impresa". Così G. SANTORO-PASSARELLI, *Diritto dei lavori*, IV edizione, Giappichelli, Torino, 2013, 279.

214 A. PERULLI fa in questo senso riferimento ad una c.d. "clausola valvola". In *Il controllo giudiziale dei poteri dell'imprenditore tra evoluzione legislativa e diritto vivente*, *Riv. it. Dir. Lav*., I, 2015, 90 ss.

215 Sulla clausola generale di correttezza e buona fede quale concetto al quale ricondurvi il perseguimento delle finalità di solidarietà sociale prescritte dagli artt. 2 e 3 comma 2 Cost. L. CASTELVETRI, *Correttezza e buona fede nella giurisprudenza del lavoro. Diffidenza e proposte dottrinali*, *Dir. Rel. Indu*., n. 2, 2001, 237 ss.

reciproca[216], realizzata al fine di un'ottimale organizzazione del lavoro e dell'ottenimento del risultato produttivo a cui è diretta[217].

È proprio nell'ottica della violazione di questa clausola generale ed elastica, relativa ai doveri di correttezza e buona fede, che si potrebbe, presumibilmente, ascrivere la condotta del lavoratore che compia un'azione di controllo sul datore di lavoro e sulle informazioni riguardanti la sua impresa, laddove la violazione dei doveri di diligenza e fedeltà (di cui agli artt. 2104 e 2105 c.c.) sia più specificamente riconducibile all'inosservanza dei doveri conformativi al potere direttivo datoriale, volto a dirigere la prestazione attraverso la puntuale delineazione delle mansioni di volta in volta convenute nel contratto e a regolare il funzionamento dell'organizzazione dell'impresa e dei rapporti che in essa e fuori di essa si svolgono[218]. Tale clausola generale, dunque, si ritiene possa porsi quale canale di recepimento delle nuove esigenze relazionali delle parti, che si dispiegano all'interno del rapporto di lavoro, derivanti dai cambiamenti delle modalità di configurazione delle reciproche esigenze e dell'assetto produttivo in cui esse operano[219].

Confacenti ai doveri direttamente discendenti dal contratto di lavoro sono gli obblighi di diligenza e fedeltà. Il primo, da un lato, individua nella natura della prestazione e nell'interesse dell'impresa i criteri attraverso cui valutare la diligenza del prestatore di lavoro (comma 1, art. 2104 c.c.), implicando che l'intensità della diligenza richiesta debba essere determinata in relazione alle mansioni d'assunzione[220] e, dall'altro, pone l'ulteriore obbligo di osservanza delle disposizioni per l'esecuzione e la disciplina del lavoro, intendendo per tali le modalità di esecuzione della

---

216 Si pone l'accento così, più che sulla messa a disposizione delle energie lavorative esigibili ed attivate dall'esercizio del potere direttivo dell'imprenditore, sull'importanza dell'aspettativa del creditore in ordine al risultato della prestazione, così che il coordinamento all'organizzazione lavorativa assume una valenza bidirezionale. La collaborazione funge, quindi, da criterio di valutazione dei comportamenti che le parti devono tenere in osservanza dei generali doveri di correttezza e buona fede. R. PESSI, *Lezioni di diritto del lavoro*, IV edizione, Giappichelli, Torino, 2010, 206.

217 C. ZOLI, *Il controllo giudiziario e gli atti di esercizio del potere direttivo: il trasferimento del lavoratore e il mutamento delle mansioni*, *Dir. Rel. Indu*., n. 3, 2014, 720 ss.; M. N. BETTINI, *Mansioni del lavoratore e flessibilizzazione delle tutele*, Giappichelli, Torino, 2014, 62, che, riprendendo M. PERSIANI, definisce il contratto di lavoro come "un'obbligazione strutturalmente aperta, cioè tale da ricomprendervi almeno potenzialmente, tutti i comportamenti collaborativi necessari alla soddisfazione dell'interesse tipico del datore di lavoro".

218 C. PISANI, che afferma che l'obbligo previsto dall'art. 1175 c.c. vada a coprire quello spazio dove non arrivano gli altri obblighi contrattuali del lavoratore, *Licenziamento e fiducia*, Giuffrè, Milano, 2004, 120.

219 Cfr. M. BROLLO, *Dignità e professionalità del lavoratore al tempo del Jobs Act*, in AA. VV., *Il diritto accessibile: non lavoro, povertà, disagio. Documenti di analisi e proposte*, 2016, 26 ss. http://www.cittadinanzattiva.it/files/notizie/giustizia/Diritto-Accessibile-Documenti-di-analisi-e-proposte-volume-unico.pdf.

220 R. PESSI, *Lezioni di diritto del lavoro*, IV edizione, Giappichelli, Torino, 2010, 260.

prestazione e le disposizioni organizzative predisposte dal datore di lavoro per la proficua utilizzazione della prestazione stessa (comma 2, art. 2104 c.c.). Il secondo obbligo (art. 2105 c.c.) sembra non avere solo un contenuto negativo, come desumibile dalla lettera della norma (non trattare affari per conto di terzi in concorrenza con l'imprenditore, né divulgare notizie attinenti all'organizzazione e ai metodi d'impresa), ma anche un contenuto positivo, che si traduce nella partecipazione attiva del lavoratore alla realizzazione del risultato voluto dal datore, assumendo così valenza anche in termini integrativi dell'obbligo di collaborazione[221].

Appare opportuna, a titolo esemplificativo, la valutazione di qualche pronuncia giurisprudenziale, la quale si sia espressa in casi sussumibili nella specifica ipotesi di un controllo, o di un'ingerenza ad esso riconducibile, operato dal lavoratore nei confronti della parte datoriale.

Innanzitutto, si può fare cenno a due recenti sentenze della Cassazione penale[222], le quali, entrambe, riconoscono il reato di accesso abusivo ad un sistema informatico o telematico, di cui all'art. 615 *ter* c.p.[223] imputabile al dipendente[224] che, pur essendo abilitato all'accesso o al mantenimento nel suddetto sistema, violi le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite

221 G. SANTORO-PASSARELLI, *Diritto dei lavori*, IV edizione, Giappichelli, Torino, 2013, 281. R. PESSI rileva che, anche se il testo dell'art. 2105 c.c. è costruito in termini di divieto di determinate condotte, la giurisprudenza ha affermarmato che questo non esaurisce l'insieme dei comportamenti che, in relazione alla varietà delle fattispecie concrete, possono essere considerati come dovuti, quale conseguenza o esplicazione del dovere di fedeltà. Rileva anche la non coicidenza di posizioni, sia in dottrina che in giurisprudenza, in ordine alla riferibilità dell'insieme di obblighi sussidiari all'obbligo di fedeltà, ovvero all'obbligo di diligenza o anche ad una clausola generale di correttezza e buona fede. In definitiva , l'obbligo di fedeltà si configurerebbe quale obbligo accessorio a quello principale relativo alla prestazione e alle modalità della sua esecuzione, connesse all'obbligo di fornire la collaborazione all'interno dell'impresa come previsto dall'art. 2094. *Lezioni di diritto del lavoro*, IV edizione, Giappichelli, Torino, 2010, 261.

222 Cass. Pen., sez. V, 13 marzo 2017, n. 11994 e Cass. Pen., sez. V, 24 marzo 2017, n. 14546.

223 Art. 615 *ter*, Accesso abusivo ad un sistema informatico o telematico: Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

224 Oltre che un reato di trattamento illecito dei dati personali di cui all'art. 167 d.lgs. 196/2003.

dal titolare del sistema (cioè dal datore di lavoro), delineate al fine di determinarne oggettivamente l'accesso, ovvero ponga in essere operazioni di natura ontologicamente differente da quelle per le quali l'accesso è consentito o dalle mansioni per le quali egli è stato assunto. Non hanno rilievo, invece, per la configurazione del reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso al sistema. In questo caso, appare evidente che il lavoratore che voglia difendersi dalle conseguenze in ambito disciplinare di una tale condotta, dovrà dimostrare di aver seguito le prescrizioni contenute in disposizioni organizzative interne, in prassi aziendali o in clausole del contratto individuale di lavoro, poiché fuori da questi binari non solo si configura un'ipotesi di inadempimento contrattuale, ma anche un illecito penale[225].

Un'altro caso, che può essere fatto rientrare nell'ipotesi di controllo del lavoratore, è quello inerente alla registrazione di conversazioni nell'ambiente di lavoro[226]. Tale fattispecie può configurare la violazione dell'obbligo di fedeltà, inteso quale obbligo complessivo del lavoratore di conformare la propria attività non solo ai caratteri della lealtà, della fiducia e della trasparenza, ma anche a quelli relativi alla correttezza e buona fede, nella compartecipazione al medesimo interesse perseguito dall'impresa. Dall'obbligo di fedeltà si ricava, inoltre, un peculiare diritto del datore di lavoro alla riservatezza delle informazioni che il suo dipendente, in ragione dell'appartenenza alla compagine organizzativa del lavoro, abbia l'occasione di assumere e ciò anche in assenza di una prescrizione specifica di riservatezza attinente alle informazioni (come avviene per i segreti aziendali)[227].

Un motivo per il quale il lavoratore sia interessato a carpire informazioni o documentazioni aziendali può individuarsi nella sua intenzione di produrre in giudizio tali informazioni, ad esempio nell'ambito di un procedimento disciplinare[228]. La giurisprudenza ha dovuto così pronunciarsi sul potenziale conflitto intercorrente tra il diritto alla riservatezza, violato dal lavoratore, e il diritto alla difesa processuale, affermando il principio della c.d. gerarchia mobile[229] dei diritti suddetti, consistente nell'attribuire al giudice il potere di valutare e di stabilire quale dei due interessi opposti sia, di volta in volta, meritevole di preferenziale protezione. In larga misura, il bilanciamento tra gli interessi in gioco si è risolto in modo da far prevalere il diritto di difesa, seppur attuato mediante la registrazione illegittima o l'abusivo impossessamento di informazioni aziendali da parte del lavoratore e la loro successiva produzione in giudizio, al fine di far valere i propri diritti.

---

225 R. GUARINIELLO, *Accesso abusivo al sistema informatico e trattamento illecito di dati personali*, *Diritto&Pratica del Lavoro*, 15/2017, 940.

226 Cass., sez. lav., 21 novembre 2013, n. 26143.

227 Diritto alla riservatezza del datore che si ricava anche dai contratti collettivi e dai codici etici di lavoro che impongono al lavoratore di mantenere riservate le informazioni assunte nello svolgimento dell'attività lavorativa.

228 Cass., sez. lav., 16 novembre 2012, n. 20163.

229 Anche Cass., sez. lav., 5 agosto 2010, n. 18279 con nota di G. Riccio, *Antagonismo fra diritto alla privacy e diritto alla difesa e criteri di bilanciamento*, Arg. Dir. lav., 2011, 172 ss.

Due recenti sentenze della Cassazione[230] hanno trattato la conflittualità che si pone tra i suddetti diritti contrapposti e l'opportunità del licenziamento per giusta causa conseguente ad una violazione dell'obbligo di fedeltà ex art. 2105 c.c. In entrambi i casi si ha un impossessamento di documentazione aziendale da parte del lavoratore, compiuto al fine di esercitare il diritto di difesa in giudizio. La Suprema Corte ha, in ogni caso, riconosciuto la prevalenza del diritto di difesa processuale rispetto alle eventuali esigenze di segretezza dell'azienda, ma ha ritenuto opportuno soffermarsi sulla valutazione inerente alla legittimità delle modalità di apprensione ed impossessamento, posto che le stesse potrebbero, di per sé, concretare ipotesi delittuose o comunque integrare la giusta causa del licenziamento per violazione dell'art. 2105 c.c., poiché si rileva che la condotta del lavoratore si sia posta in contrasto con i criteri comportamentali imposti dal dovere di fedeltà e dalla clausola generale di correttezza e buona fede, in modo tale da ledere irreversibilmente il rapporto fiduciario intercorrente tra le parti. Dunque, la Corte ha fatto emergere la necessità di operare una distinzione tra l'attività di produzione in giudizio dei documenti aziendali riservati al fine di esercitare il diritto alla difesa e l'attività di impossessamento dei documenti aziendali, eventualmente prodromica alla successiva produzione dei medesimi. Tale questione deve essere risolta tenendo sempre presente la possibilità di ravvisare, nell'esercizio del diritto di difesa, una scriminante della condotta posta in essere dal lavoratore[231].

In questa analisi circa l'opportunità o meno di un eventuale attività di controllo messa in atto dal lavoratore sul datore di lavoro e sulle informazioni riservate relative all'azienda e le sue possibili conseguenze, sia nell'ambito del rapporto lavorativo che in quello processuale, è stato sempre messo in luce il lato illegittimo di una tale attività, la quale si è supposto venga eseguita occultamente e contrariamente ai doveri di diligenza e fedeltà, in quanto compiuta al di là delle mansioni e delle prescrizioni espressamente previste e delineate dal datore di lavoro nel contratto, tanto da andare a scalfire quello che è l'elemento su cui si costruisce la relazione lavorativa, ossia la fiducia, in un mancato rispetto anche dell'intento di collaborazione in vista del risultato produttivo.

A questo punto è possibile accennare ad una peculiare forma di controllo sull'attività e sull'andamento dell'azienda e del datore di lavoro prevista espressamente dalla legge e quindi assolutamente legittima. Si fa riferimento all'opera del rappresentante dei lavoratori per la

230 Cass., sez. lav., 13 luglio 2016, n. 14305; Cass., sez. lav., 8 agosto 2016, n. 16629.

231 Nei motivi della decisione di ambedue le sentenze si afferma che "il lavoratore che produca, in una controversia di lavoro intentata nei confronti del datore di lavoro, copia di atti aziendali, che riguardino direttamente la sua posizione lavorativa, non viene meno ai doveri di fedeltà di cui all'art. 2105 c.c., tenuto conto che l'applicazione corretta della normativa processuale in materia è idonea ad impedire una vera e propria divulgazione della documentazione aziendale e che, in ogni caso, al diritto di difesa in giudizio deve riconoscersi prevalenza rispetto alle eventuali esigenze di segretezza dell'azienda". Così a partire da Cass. n. 6420/2002, poi Cass. n. 22923/2004, Cass. n. 3038/2011, Cass. n. 12119/2012, Cass. 6501/2013, Cass. n. 25682/2014.

sicurezza[232] (RLS), il cui compito è, in generale, quello di monitorare l'attività aziendale con particolare interessamento rivolto alle questioni della salute e della sicurezza sul lavoro.

Al fine di agevolare lo svolgimento delle funzioni di controllo che il Legislatore ha attribuito ai rappresentanti dei lavoratori per la sicurezza, l'art. 50 del d.lgs. 81/2008 (Testo Unico in materia di sicurezza sul lavoro) riconosce espressamente un diritto di accesso non solo ai luoghi in cui si svolgono le lavorazioni, ma anche ai dati di cui all'art. 18 co. 1 lett. r)[233] contenuti in applicazioni informatiche[234].

Il diritto di accesso qui contemplato non può essere del tutto assimilabile ad una forma di controllo a distanza, ma configura pur sempre un esempio di controllo (legittimo) operato dalla parte debole del rapporto di lavoro a suo vantaggio, nella prospettiva di un'ottimale realizzazione della relazione lavorativa.

La regolamentazione collettiva prevede, peraltro, la segnalazione preventiva delle visite e degli accessi che si intendono effettuare. Tuttavia, il diritto di accesso, in quanto qualificabile come diritto potestativo, non è subordinato al previo assenso del datore di lavoro e, in mancanza di vincoli procedurali stabiliti dalla contattazione collettiva, incontra i soli limiti posti dall'ordinamento per impedire forme illegittime di esercizio dello stesso[235]. Circa il rispetto delle esigenze produttive, contemplato dalla disciplina collettiva, questo non può tradursi in una forma astratta dietro la quale possa trincerarsi il datore di lavoro per ostacolare l'attività del rappresentante, anche perché egli è tenuto a dimostrare l'esistenza di tali esigenze[236].

Ciò che si rileva è che il d. lgs. 81/2008, e nello specifico l'art. 50, nel tentativo di rafforzare l'effettività del sistema prevenzionale nell'ambito lavorativo, abbiano confermato la centralità del ruolo attribuito ai lavoratori all'interno di una dimensione collettiva, anche per il tramite di un'azione (seppur circoscritta) di verifica e controllo esercitati sul datore di lavoro, sulla sua attività e su determinate informazioni a questa relative.

---

232 In base alla legge 626/1994 **il** Rappresentante dei lavoratori per la sicurezza è *la persona eletta o designata per rappresentare i lavoratori per quanto concerne gli aspetti della salute e della sicurezza durante il lavoro.*

233 Il RLS ha i diritto di accedere ai dati e alle informazioni relative agli infortuni sul lavoro "che comportino l'assenza del lavoratore di almeno un giorno, escluso quello dell'evento, e, ai fini assicurativi, quelli relativi agli infortuni sul lavoro che comportino un'assenza dal lavoro superiore a tre giorni".

234 In questo modo è stato sostituito l'obbligo di tenuta del registro infortuni di cui all'art. 4, co. 5, lett. o) d.lgs. 6626/1994.

235 Già Cass., sez. lav., 13 settembre 1982, n. 4874.

236 C. ZOLI, *La nuova sicurezza sul lavoro, I Principi comuni*, Commentario diretto da L. MONTUSCHI, Zanichelli, Bologna, 2011, 507 ss.

5. Il sindacato e l'impiego delle nuove tecnologie dell'informazione e della comunicazione. Brevi riflessioni.

Lasciando il discorso su una dimensione collettiva, ci si può interrogare, a questo punto, sui ruoli assunti dalle parti sociali nelle dinamiche contrattualistiche e concertative all'esito dell'avvento *lato sensu* della tecnologia digitale e dell'informazione nel mondo del lavoro. Soprattutto ci si interroga se la parte sociale rappresentata dai sindacati sia stata e sia, al momento, capace di recepire il cambiamento e di reagire e sfruttare a suo vantaggio le (eventuali) opportunità offerte dalle dinamiche che sottendono all'industria 4.0[237] ed alla condivisione di informazioni innescata dalle tecnologie dell'informazione e della comunicazione (ICT), magari nel tentativo di riscattarsi dalla posizione di debolezza in cui si trova nei rapporti di forza nei confronti dell'altra parte sociale, quella datoriale.

È opportuna una preliminare considerazione circa il quadro apportato negli ultimi anni dal progresso tecnologico, ed in particolar modo dall'impatto della diffusione delle ICT sulle dinamiche occupazionali e salariali osservabili nei mercati del lavoro dei Paesi industrializzati, a fronte della sorprendente accelerazione del progresso delle nuove tecnologie e del contestuale declino dei costi di produzione, elementi considerati alla base della *digital economy*.

In termini sintetici, il quadro presenta, da un lato, il contributo positivo delle ICT alla produttività dei settori che investono in innovazione e dei settori che si dedicano agli investimenti complementari relativi all'innovazione organizzativa e alla formazione di personale qualificato, oltre che alla espansione del mercato dei cd. beni digitali[238] e, dall'altro, il contributo

237 L'espressione *Industria 4.0* è collegata alla c.d. "quarta rivoluzione industriale". Resa possibile dalla disponibilità di sensori e di connessioni *wireless* a basso costo, questa nuova rivoluzione industriale si associa a un impiego sempre più pervasivo di dati e informazioni, di tecnologie computazionali e di analisi dei dati, di nuovi materiali, componenti e sistemi totalmente digitalizzati e connessi (*internet of things and machines*). I principali paesi industrializzati si sono già attivati a supporto dei settori industriali nazionali in modo da cogliere appieno quest'opportunità. L'Italia ha sviluppato un "Piano nazionale Industria 4.0 2017-2020" che prevede misure concrete in base a tre principali linee guida: operare in una logica di neutralità tecnologica; intervenire con azioni orizzontali e non verticali o settoriali; agire su fattori abilitanti. http://www.sviluppoeconomico.gov.it/index.php/it/industria40.

238 Per "beni digitali" si intende l'insieme dei beni e servizi convertibili in un flusso di *bit*. Questi si distinguono dai beni tradizionali poiché caratterizzati da costi marginali di produzione prossimi allo zero e da una crescita del loro consumo (si pensi alla tecnologia degli *user generated contents*, ove il materiale consumato viene caricato e condiviso dagli utenti, come ad esempio accade con You Tube o Wikipedia, o alle tecnologie di comunicazione telematica). Cfr. E. BRYNJOLFSSON, A. MCAFEE, *La nuova rivoluzione delle macchine. Lavoro e prosperità nell'era della tecnologia trionfante*, Feltrinelli, Milano, 2015.

potenzialmente negativo sui livelli occupazionali[239]. Saranno i *policy makers* a dover fare i conti con questi importanti cambiamenti strutturali delle dinamiche economiche e lavorative, i quali solo attraverso un'adeguata comprensione di tali fenomeni e delle tendenze da essi innescate potranno essere in grado di determinare quanta parte del progresso legato alle ICT andrà a migliorare le prospettive economiche e quanta parte invece comporterà perdite di benessere, in termini di abbassamento salariale e disoccupazione tecnologica[240].

In Italia, non sembra che vi sia una reale comprensione della questione da parte della politica e dei sindacati, i quali non sembrano ancora adeguatamente preparati alla sfida che il cambiamento porta con sé. Eppure qualcosa si sta muovendo in tale direzione, soprattutto in termini di riconoscimento del problema ed analisi di modelli di riferimento, anche se le discussioni in merito sono ancora per lo più ignorate dalla gran parte dell'opinione pubblica, la quale non pare essere, al momento, sufficientemente coinvolta ed informata dalle forze politiche e sindacali.

Un primo segnale di una effettiva presa di coscienza del fenomeno è rappresentato da un *draft* presentato il 13 marzo 2017 al governo da parte di Cgil, Cisl e Uil, intitolato "Una via italiana a Industria 4.0 che guardi ai modelli europei più virtuosi"[241], nel quale si delineano ipotesi di opportunità e di priorità inerenti al mercato economico e del lavoro[242], senza però la presentazione di proposte concrete atte a delineare una prima soluzione ai numerosi punti critici.

A livello europeo si è svolto un recente dibattito[243] inerente alle condizioni dei lavoratori della c.d. *gig-economy*[244] e al problema del precariato digitale, nel quale si è prospettata la necessità di garantire gli elementi di protezione sociale basilari per tali lavoratori.

---

239 A tal proposito è stata rilevata la presenza concreta di un rischio di computerizzazione, intendendo dire con tale espressione che parte delle occupazioni attualmente svolte da esseri umani finiranno per essere assegnate a computer e a intelligenze artificiali. C. B. FREY, M. A. OSBORNE, *The future of employment: how susceptible are jobs to computerisation*, 2013, http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf.

240 Espressione coniata nel 1930 da J. M. KEYNES, per il quale la disoccupazione tecnologica assumeva i contorni di una malattia. Si tratta di una disoccupazione causata dalla scoperta di nuovi mezzi per risparmiare sull'utilizzo del lavoro a una velocità superiore a quella con la quale si riesca a trovare nuove forme di impiego.

241 http://www.uil.it/documents/130317%20INDUSTRIA%204_0.pdf.

242 Quali la determinazione di una nuova gestione delle dinamiche occupazionali, l'opportunità della formazione di competenze adeguate e la riorganizzazione e redistribuzione degli orari di lavoro.

243 Dibattito avviato dalla Commissione nell'aprile 2017 e che ha avuto quale esito la delineazione degli European Pillar of Social Rights , contenenti una serie di principi chiave e diritti relativi ad un giusto ed equo mercato del lavoro.

244 Per *gig economy* (dove gig sta per lavoretto) si intende un modello economico dove non esistono più le prestazioni lavorative continuative (il posto fisso, conntratto a tempo indeterminato) ma si lavora *on demand*, cioè solo quando c'è richiesta per i propri servizi, prodotti o competenze. Domanda e offerta vengono gestite *online* attraverso piattaforme e app dedicate. I lavoratori sono tutti in proprio e svolgono attività cottimizzate temporanee e non continuative. *Si pone in*

Alla luce di ciò, si constata che, in realtà, il tema della partecipazione del sindacato e dei lavoratori ai processi organizzativi e di *governance* delle imprese si pone come sempre più attuale, in seguito alle grandi trasformazioni in atto nel sistema sociale e produttivo. Tuttavia, l'importanza del ruolo che il sindacato potrebbe e dovrebbe rivestire in questo momento storico si scontra con l'inadeguatezza delle sue forme di intervento, divenute sempre più deboli dopo la crisi economica, configurando una voce sempre più inascoltata nel panorama politico.

A questo riguardo si può ipotizzare che i sindacati, mediante l'impiego della tecnologia dell'informazione e della comunicazione, possano assumere un ruolo di maggior forza nelle dinamiche contrattuali e concertative, in virtù della maggiore divulgazione ed informazione sui programmi e sulle proposte relative alle nuove problematiche del mondo del lavoro, aggregando il più possibile cerchie di lavoratori differenti tra loro per mansioni e tipologia di attività, ma sempre più simili per le precarie condizioni lavorative[245]. Si auspica, in questo modo, la creazione di una voce lavorativa comune idonea ad avere maggior peso politico e atta a ricevere maggiore attenzione dall'opinione pubblica. Ciò potrebbe realizzarsi attraverso l'uso della rete e soprattutto attraverso personale sindacale impiegato in un ruolo lavorativo che potrebbe essere assimilabile a quello del *social media marketing*, il quale si occuperebbe non solo di divulgazione e diffusione del messaggio politico e della linea propria dello specifico sindacato, ma anche presterebbe costante attenzione alle problematiche concrete e contingenti poste dagli iscritti.

Come per il fenomeno dell'attivismo digitale[246] anche per l'attività sindacale la rete potrebbe assumere i contorni di una nuova piazza ove manifestare, diffondere e concretizzare la propria opera.

Tali considerazioni muovono anche alla luce del recente episodio che ha visto quali protagonisti un autista dell'azienda Uber ed il ceo dell'azienda, il quale è stato ripreso con una videocamera nascosta dal suo dipendente, durante un passaggio nella sua vettura, mentre esprimeva, laconicamente ma in modo esplicito, le sue considerazioni circa le condizioni di lavoro e salariali dei lavoratori dell'azienda lamentate proprio dall'autista. Il punto interessante della vicenda è stato che in seguito alla divulgazione in rete da parte del dipendente del video della conversazione tra lui ed il ceo, la questione inerente alle condizioni salariali dei lavoratori della suddetta azienda abbia avuto un risalto a livello globale, oltre che la successiva presentazione pubblica delle proprie scuse

---

una zona grigia tra il lavoro da freelance e quello da dipendente, poiché comunque ci sono indizi di subordinazione come il fatto di avere dei turni o il potere disciplinare, che può avere quale esito l'estromissione.

245 Si pensi alla posizione precaria non solo dei lavoratori impiegati per lavori manuali ma anche delle professioni intellettuali, quali i liberi professionisti.

246 Par. 3.1, cap. 2.

da parte dell'amministratore delegato[247]. L'episodio vuole essere solo un esempio relativo al potere che la maggiore diffusione della voce dei lavoratori e dei loro rappresentanti potrebbe avere attraverso l'impiego della rete, fino ad arrivare ad ipotizzare un rinnovato equilibrio se non addirittura, in alcuni casi, un ribaltamento delle tradizionali forze imputabili alle parti sociali nel dibattito contrattuale e politico, a vantaggio di quella dei lavoratori.

In conclusione, si rileva la necessità di un'urgente presa di coscienza, delle nuove dinamiche interne al mondo del lavoro, in termini di *policy making* da parte delle parti sindacali, oltre che l'auspicio di una nuova conquista dell'opportuno ruolo di risalto che spetterebbe al sindacato nel dibattito e nella formulazione di proposte atte ad avere un più vasto ed incisivo riverbero a livello politico e contrattuale, nella determinazione di un maggior controllo sui rapporti di forza che si innescano tra le parti sociali in termini di effettività delle prerogative dei lavoratori nei confronti della controparte datoriale. Il ruolo della contrattazione collettiva, a tutti i livelli, dovrà essere necessariamente di sostegno e di governo di tali processi affinché, nel mondo del lavoro, non si assista ad un aumento delle diseguaglianze e della disoccupazione.

247 https://www.theguardian.com/technology/2017/feb/28/uber-ceo-travis-kalanick-driver-argument-video-fare-prices.

Conclusioni.

Si è visto, nella prima parte dell'elaborato, che le ragioni della riforma dell'art. 4 Stat. Lav., siano da ravvisarsi nella obsolescenza della disciplina statutaria determinata dall'avvento delle nuove tecnologie, che si sono velocemente imposte nell'ambito lavorativo, e nella ricerca di una maggiore tutela da attribuire al diritto alla riservatezza della persona-lavoratore, alla luce sia della pervasività nella sfera anche privata determinata dall'impiego di tali strumenti tecnologici e sia dell'evoluzione della normativa generale relativa alla tutela della *privacy*, compiuta a partire dall'emanazione del d.lgs. 30 giugno 2003, 196 ed integrata attraverso i provvedimenti man mano delineati dal Garante. Tant'è che una delle innovazioni recate dalla modifica consiste proprio nell'intreccio tra la normativa lavoristica e la normativa della *privacy* e, dunque, nel necessario adeguamento della prima altresì agli interventi valutativi e prescrittivi del Garante, che si connotano per una costante puntualità ed attualità.

In questo modo, la tutela della riservatezza del lavoratore viene garantita attraverso un'attenzione più coerente alla dimensione individuale, più confacente a tale tutela, attraverso la previsione di una maggiore trasparenza dei controlli, dei quali il lavoratore deve avere adeguata informazione, e la compenetrazione dei limiti posti ai suddetti controlli dalla normativa lavoristica con i limiti generali previsti dalla disciplina della *privacy*.

Una delle novità apportate è, innanzitutto, quella dell'eliminazione del divieto esplicito di effettuazione dei controlli a distanza sull'attività lavorativa, che ci si è accorti essere prettamente un cambiamento formale più che sostanziale, per quanto possa sottendere alcune ragioni metagiuridiche idonee a far ipotizzare una messa in luce non più dell'atto vietato, ma solo della regolazione dei casi in cui tale atto sia consentito. Tuttavia, dal punto di vista sostanziale, il divieto, seppur implicito, permane, confermando la volontà del Legislatore di assoggettare il controllo a limiti specifici, individuati nelle esigenze aziendali e nella previa ricerca dell'accordo sindacale o dell'autorizzazione amministrativa.

In secondo luogo, altre due significative novità si è visto essere quelle relative, da un lato, la previsione, tra le ragioni aziendali legittimanti il controllo, della tutela del patrimonio aziendale, nell'intento di superare l'annosa diatriba sui controlli difensivi e determinando la necessità di una rinnovata qualificazione degli stessi e, dall'altro, la scelta legislativa di ritenere esonerato da ogni condizione di legittimità l'impiego degli strumenti utilizzati per rendere la prestazione lavorativa, oltre che degli strumenti di registrazione degli accessi e delle presenze.

Infine, l'aspetto probabilmente più rilevante della riforma ha riguardato la facoltà concessa al datore di lavoro di raccogliere, attraverso gli strumenti dai quali derivi un controllo, e di utilizzare le informazioni a tutti i fini connessi al rapporto di lavoro, dunque anche a fini disciplinari.

Ciò premesso, dall'analisi del riformato art. 4 Stat. Lav. è emersa evidente l'importanza del bilanciamento che deve essere operato tra i contrapposti interessi del datore di lavoro a ricevere la corretta prestazione a lui dovuta e alla verifica, legittima, affinché questa venga adempiuta nel modo dovuto e del lavoratore a vedere riconosciuta la tutela dei suoi diritti di dignità e riservatezza.
Dalla ricerca di questo delicato equilibrio si è giunti, dunque, a rilevare che la vigilanza attuata sul lavoratore, ancorchè necessaria nell'organizzazione produttiva, debba essere mantenuta in una dimensione umana, ossia non esasperata dall'uso di tecnologie suscettibili di rendere l'opera di monitoraggio continua ed anaelastica, suscettibile, in questo modo, di eliminare ogni zona di riservatezza e di autonomia nello svolgimento del lavoro.
A seguito della nuova disciplina sui controlli a distanza si è anche constatato come la posizione del datore di lavoro abbia acquisito una maggiore complessità in ragione del ruolo da lui assunto nella relazione lavorativa. Infatti il nuovo testo dell'art. 4 non ha affatto semplificato la vita del datore di lavoro, poiché si configura come opportuna una chiara e specifica consapevolezza della propria organizzazione aziendale ed una comprensione dei profili tecnici e delle loro conseguenze giuridiche. In concreto, questa è la consapevolezza che deve essere impiegata dal datore di lavoro nell'installazione ed utilizzo degli strumenti di controllo a distanza e nella rilevazione della differenza intercorrente tra strumento di controllo e strumento di lavoro e poi trasfusa nell'informativa sul trattamento dei dati, che deve essere tale da fornire un'adeguata informazione al lavoratore circa le modalità d'uso dei suddetti strumenti e l'effettuazione dei controlli, pur sempre nel rispetto della disciplina sulla *privacy*.
Un'ultima analisi, in questa prima parte, è stata rivolta alla disciplina del controllo a distanza in virtù dell'impiego dei *social network* ed in relazione al fenomeno dello *smart working*, con la considerazione della necessità del rispetto, anche in questi casi, di entrambe le normative sia lavoristica che di tutela della *privacy*, oltre che alla constatazione del consolidarsi di un sistema in cui vita lavorativa e vita privata si intrecciano e si confondono, determinando l'incapacità concettuale e giuridica di separare e definire il tempo del lavoro ed il tempo libero. Separazione e definizione che sarebbero funzionali a soddisfare quel giusto diritto alla disconnessione, che coinvolge e tutela tanto l'ambito lavorativo quanto quello privato della persona-lavoratore.
In questa sede si è voluto, dunque, oltre che far emergere le novità scaturenti dalla normativa *post* riforma, provare ad individuare le ragioni e le conseguenze del cambio di prospettiva da questa generato, attuato sì dal Legislatore, ma ovviamente innescato dall'evoluzione della società e dalle nuove e non ancora compiutamente delineate esigenze di *privacy* anche digitale dell'individuo.
Nella seconda parte dell'elaborato si è provato ad analizzare il fenomeno del controllo potenzialmente attuabile mediante la tecnologia digitale ed informatica da parte di chiunque,

nell'ottica di giungere al vaglio dell'ipotesi di un possibile controllo messo in atto dal lavoratore sul datore di lavoro ed alla seguente valutazione di una sua (in)opportunità.

In particolare, si è partiti dall'assioma secondo il quale maggiore è la tecnologia impiegata nella registrazione e catalogazione delle informazioni, maggiore sarà la vulnerabilità di questa al controllo e dalla constatazione della intrinsecità della facoltà di effettuare un'azione di controllo all'impiego di uno strumento informatico, per poi giungere alla considerazione che l'intuitività d'uso dello strumento e la sua ampia disponibilità siano tali da creare l'opportunità del compimento di una tale azione, in un meccanismo per il quale sia il mezzo a giustificare il fine.

In virtù di tale premessa, dunque, si deduce che anche il lavoratore potrebbe compiere una tale azione di controllo rivolta al suo datore di lavoro.

Situazione questa che viene stimata, alla luce della normativa determinante i doveri delle parti nel rapporto di lavoro e nella relazione contrattuale ad esso sottesa, come corrosiva di quello che è l'elemento su cui si costruisce la relazione lavorativa, ossia la fiducia.

Anche la giurisprudenza ha apportato un contributo in materia, in particolare, mettendo a confronto il diritto alla difesa del lavoratore, nell'eventualità in cui abbia carpito informazioni appartenenti alla parte datoriale al fine di far valere in giudizio un suo diritto, e il diritto alla riservatezza del datore di lavoro circa le informazioni e i documenti relativi alla sua attività, e delineando, a riguardo, una c.d. gerarchia mobile dei diritti suddetti, consistente nell'attribuire al giudice il potere di valutare e di stabilire quale dei due interessi opposti sia, di volta in volta, meritevole di preferenziale protezione.

Infine, si è voluto operare una sorta di parallelismo circa il valore che può assumere il mezzo tecnologico dell'informazione e della comunicazione al fine di apportare cambiamenti di carattere politico e sociale, sia nell'ambito politico e sia nell'ambito sindacale. Cambiamenti che vengono apportati dalle azioni compiute dagli attivisti digitali e che si presume possano essere compiute anche dai sindacati, a condizione di una loro maggiore presa di coscienza e comprensione delle nuove realtà in cui si dispiega il contemporaneo mondo del lavoro.

Sicuramente il progresso tecnologico apporta e continuerà ad apportare, in questa sua evoluzione esponenziale, radicali cambiamenti in ambito lavorativo, i quali, si auspica, possano essere sempre ricondotti, grazie all'opera interpretativa, in una dimensione di consapevolezza del necessario bilanciamento che deve, in ogni caso, essere condotto in virtù della considerazione della persona del lavoratore, non trascurando i suoi diritti fondamentali di dignità e riservatezza.

Bibliografia.

AGAMBEN G., *Che cos'è il contemporaneo?*, Milano, Nottetempo edizioni, 2008.

AGAMBEN G., *Che cos'è un dispositivo?*, Milano, Nottetempo edizioni, 2006.

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

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. 2, n. 1, 2016.

AMATO V., *Legittimità del controllo difensivo occulto attraverso i social networks*, in *il Lavoro nella giurisprudenza*, 10/2015, 896.

BARRACO E:, SITZIA A., *La tutela della privacy nei rapporti di lavoro*, Milano, Ipsoa, 2012.

BARRACO E., SITZIA A., *Potere di controllo e privacy*, Milano, Wolters Kluwer, 2016.

BELLAVISTA A., *Il controllo sui lavoratori*, Torino, Giappichelli, 1995.

BELLAVISTA, *Gli accordi sindacali in materia di controlli a distanza sui lavoratori,* in *il Lavoro nella giurisprudenza*, 2014, 737.

BETTINI M. N., *Mansioni del lavoratore e flessibilizzazione delle tutele*, Torino, Giappichelli, 2014.

BONATO B., *La possibilità della discrezione*, in (a cura di) BONATO B. *La trasparenza e il segreto*, Milano-Udine, Mimesis edizioni, 2017.

BROLLO M., *Dignità e professionalità del lavoratore al tempo del Jobs Act*, in AA. VV., *Il diritto accessibile: non lavoro, povertà, disagio. Documenti di analisi e proposte*, 2016, in

http://www.cittadinanzattiva.it/files/notizie/giustizia/Diritto-Accessibile-Documenti-di-analisi-e-proposte-volume-unico.pdf.

BRYNJOLFSSON E., MCAFEE A., *La nuova rivoluzione delle macchine. Lavoro e prosperità nell'era della tecnologia trionfante*, Milano, Feltrinelli, 2015.

CARINCI F., *Rivoluzione tecnologica e diritto del lavoro*, in *Giornale di diritto del lavoro e delle relazioni indu*striali, 1985, 224.

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, n. 1, 2016.

CASTELLANETA M., *Email aziendale: il controllo è una ingerenza sulla vita privata, ma se c'è un divieto consapevole può essere ammesso*, in *Guida al Diritto*, n. 7, 2016, 112.

CASTELVETRI L., *Correttezza e buona fede nella giurisprudenza del lavoro. Diffidenza e proposte dottrinali*, in *Diritto delle Relazioni Industriali*, n. 2, 2001, 237.

CERBERUS, Soluzione antifurto per Android, in https://www.cerberusapp.com/

CERTNAZIONALE, Minacce: come evitare gli attacchi di phishing e Social Engineering, *in https://www.certnazionale.it/documenti/2015/03/02/minacce-come-evitare-gli-attacchi-phishing-social-engineering/*

CGIL, CISL, UIL, *Una via italiana a Industria 4.0 che guardi ai modelli più virtuosi*, in http://www.uil.it/documents/130317%20INDUSTRIA%204_0.pdf.

COMMISSARIATO DI P.S. *online*, Approfondimenti *Cyberstalking*, in http://www.commissariatodips.it/approfondimenti/cyberstalking.html

COMMISSARIATO DI P.S. *online*, Approfondimenti *Phishing*, in https://www.commissariatodips.it/approfondimenti/phishing.html

COSATTINI L. A., *Le modifiche all'art. 4 Stat. Lav. Sui controlli a distanza, tanto rumore; per nulla?*, in *il Lavoro nella giurisprudenza*, 11/2015, 985.

DAGNINO E., *Tecnologie e controlli a distanza,* in *Diritto delle Relazioni Industriali*, n. 4, 2015, 988.

D'ARCANGELO L., *I controlli a distanza dopo il Jobs Act. Dallo Statuto dei lavoratori alla disciplina sulla protezione dei dati personali*, in *Massimario di Giurisprudenza del Lavoro*, n. 10, 2016, 638.

DEL NINNO A., *In vigore la riforma dell'art. 4 dello Statuto dei Lavoratori sui controlli a distanza: il decreto legislativo 14 Settembre 2015 n. 151, privacy dei lavoratori e nuove regole*, *Diritto e Giustizia*, 2015.

DEL NINNO, *La riforma dell'art. 4 dello Statuto dei Lavoratori e i controlli a distanza alla luce delle nuove disposizioni di attuazione del Jobs Act: quali rischi per la privacy dei lavoratori?*, *Diritto e giustizia*, 2015.

DEL PUNTA R., *La nuova disciplina dei controlli a distanza sul lavoro (art.23, D. lgs. n. 151/2015)*, in *Rivista Italiana di Diritto del Lavoro*, 2016, 77.

DI FRANCESCO M., *Controllo a distanza e utilizzazione di impianti Gps*, in *Diritto & Pratica del Lavoro*, 10/2017, 585.

FREY C. B., OSBORNE M. A., *The future of employment: how susceptible are jobs to computerisation*, 2013, in http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf.

GALDIERI P., *Teoria e pratica nell'interpretazione del reato informatico*, Milano, Giuffrè, 1997.

GALLO P., *Contratto e buona fede. Buona fede in senso oggettivo e trasformazioni del contratto*, Torino, Utet, 2014.

GAMBA C., *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove* , *Labour&Law Issues*, vol. 2, n. 1, 2016.

GARANTE per la protezione dei dati personali, Provv. n. 303 del 13 luglio 2016, doc. web n. 5408460, in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5408460

GARANTE per la protezione dei dati personali, Provv. n. 547 del 22 dicembre 2016, doc. web n. 5958296, in http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/5958296

GARANTE per la protezione dei dati personali, Relazione annuale 2010, in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1819504

GHEZZI G., ROMAGNOLI U., *Il rapporto di lavoro*, terza edizione, Bologna, Zanichelli, 1995.

GOFFREDO M. T., MOSCA V., *Jobs Act e nuovi controlli a distanza*, in *Diritto & Pratica del Lavoro*, 31/2016, 1894.

GUARINIELLO R., *Accesso abusivo al sistema informatico e trattamento illecito di dati personali*, in *Diritto & Pratica del Lavoro*, 15/2017, 940.

HOBBES T., *Leviatano (1651)*, BUR Rizzoli, Milano, 2011.

IAQUINTA F., INGRAO A., *Il datore di lavoro e l'inganno di Facebook*, in *Rivista Italiana di Diritto del Lavoro*, 2014, 82.

IAQUINTA F., INGRAO A., *La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*, in *Diritto delle Relazioni Industriali*, 2014, 1027.

ICHINO P., *Il contratto di lavoro*, Vol. 3, Milano, Giuffrè, 2003.

INGRAO A., *Il controllo a distanza effettuato mediante Social network*, *Labour&Law Issues*, vol. 2, n. 1, 2016.

KALI LINUX, Official Documentation, in http://it.docs.kali.org/introduction-it/che-cosa-e-kali-linux

KASPERSKY Lab Daily, *Cosa sono gli exploit e perché fanno così paura*, in https://blog.kaspersky.it/exploits-problem-explanation/6393/

LAMBERTUCCI P., *Potere di controllo del datore di lavoro e tutela dellla 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", 235/2015.

LEVI A., *Il controllo informatico sull'attività del lavoratore*, Torino, Giappichelli, 2013.

MAIO V., *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *Argomenti di Diritto del Lavoro*, 6/2015, 1186.

MARAZZA M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in WP CSDLE "Massimo D'Antona", 300/2016.

MARCHESI G., *Mail aziendale e messaggi privati: la sentenza CEDU*, in *Glob.Press*, 2016.

MARESCA, *Jobs Act, come conciliare il potere di controllo e tutela della dignità e riservatezza del lavoratore*, in *Forum Tuttolavoro*, 2016.

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

MARZANO G., *Il lato maligno del Web*, Milano-Udine, Mimesis edizioni, 2016.

MC CLURE S., SCAMBRAY J., KURTZ G., *Hacker! 7.0 Nuove tecniche di protezione*, Milano, Apogeo editore, 2013.

MINISTERO DELLO SVILUPPO ECONOMICO, *Piano nazionale Industria 4.0*, in http://www.sviluppoeconomico.gov.it/index.php/it/industria40.

MINISTERO DEL LAVORO E DELLE POLITICHE SOCIALI, Risposta ad Interpello, Prot. n. 2975, 5 dicembre 2005, in

http://sitiarcheologici.lavoro.gov.it/AreaLavoro/Vigilanza/Documents/AttivitaIspettiva/37Roma302605.pdf

MINISTERO DEL LAVORO E DELLE POLITICHE SOCIALI, Comunicato stampa del 18 giugno 2015, in http://www.lavoro.gov.it/stampa-e-media/Comunicati/Pagine/20150618-Controlli-a-distanza.aspx

MIT Technology Review, *Innovators under 35*, 2010, in www2.technologyreview.com/tr35/profile.aspx?TRID=947

NATALI, A. I., *Jobs Act e legittimità del controllo a distanza dei lavoratori*, in *Diritto & Pratica del Lavoro*, 34-35/2015, 1980.

NATALI P. J., *Navigazione Internet dei lavoratori e tutela della privacy*, in *Diritto & Pratica del Lavoro*, 32-33/2015, 1917.

OGRISEG C., *Il Regolamento UE n.2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, in *Labour&Law Issues*, vol. 2, n. 2, 2016.

OLIMPIA POLICELLA E., *Controlli dei dipendenti: gli impianti audiovisivi nel nuovo art. 4 dello Statuto dei lavoratori*, *Diritto24*, 2015, in http://www.diritto24.ilsole24ore.com/art/dirittoLavoro/2015-09-15/controlli-dipendenti-impianti-audiovisivi-nuovo-art-4-statuto-lavoratori—161229.php.

PARODI C., *VoIP, Skype e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazioni?*, in *Diritto penale e processo*, 2008, 1309.

PASSAGLIA P., *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in *Consulta online*, fasc. 3, 2016, http://www.giurcost.org/studi/passaglia7.pdf.

PERSIANI M., *Diritto sindacale*, sedicesima edizione, Padova, Cedam, 2015.

PERSIANI M., *Fondamenti di diritto del lavoro*, seconda edizione, Padova, Cedam, 2015.

PERULLI A., *Il potere direttivo dell'imprenditore*, Milano, Giuffè, 1992.

PERULLI A., *Il controllo giudiziale dei poteri dell'imprenditore tra evoluzione legislativa e diritto vivente*, in *Rivista Italiana di Diritto del Lavoro*, I, 2015, 90.

PESSI R., *Lezioni di diritto del lavoro*, quarta edizione, Torino, Giappichelli, 2010.

PISANI C., *Licenziamento e fiducia*, Milano, Giuffrè, 2004.

POPOLI A. R., *Social network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *il Diritto dell'informazione e dell'informatica*, 2014, 981.

RAIMONDI F., *La riservatezza del lavoratore tra innovazioni legislative e giurisprudenza nazionale ed europea*, in *Rivista giuridica del lavoro*, 2/2016, 148.

RAUSEI P., *La nuova disciplina dei controlli a distanza fra luci e ombre*, in *Diritto & Pratica del lavoro*, 2015, 2149.

ROCCHETTI P., *I limiti al potere di controllo del datore di lavoro sulle condotte del lavoratore. Commento alle sentenze n. 22662/16 e 22213/16 della Cassazione*, *Questione Giustizia*, 2017.

RODOTÀ S., *Tecnologie e diritto*, Bologna, Il Mulino, 1995.

RODOTÀ S., *Intervista su privacy e libertà*, Bari, Laterza, 2005.

RONDO A., *I controlli sulla posta elettronica del dipendente e l'art. 4 Stat. Lav. Prima e dopo il Jobs Act*, in *Massimario di Giurisprudenza del Lavoro*, 2016, 41.

ROTONDI F., *Diritto alla disconnessione del lavoratore: non è necessario "per legge"*, *Ipsoa Wolters Kluwer*, 2017, in http://www.ipsoa.it/documents/lavoro-e-previdenza/rapporto-di-lavoro/quotidiano/2017/05/20/diritto-alla-disconnessione-del-lavoratore-non-e-necessario-per-legge.

SALAZAR P., *Facebook e rapporto di lavoro: a che punto siamo*, in *il Lavoro nella giurisprudenza*, 2/2016, 201.

SALIMBENI M. T., *La riforma dell'art. 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in *Rivista Italiana di Diritto del Lavoro*, n. 4, 2015, 589.

SANTONI F., *Controlli difensivi e tutela della privacy dei lavoratori*, in *Giurisprudenza italiana*, 2016, 146.

SANTORO-PASSARELLI G., *Diritto dei lavori*, quarta edizione, Torino, Giappichelli, 2013.

SARTOR G., *L'informatica giuridica e le tecnologie dell'informazione*, seconda edizione, Torino, Giappichelli, 2010.

SERVIDIO S., *Controllo dei dipendenti e difesa del patrimonio aziendale*, in *Diritto & Pratica del Lavoro*, 12/2016, 769.

SINZHEIMER H., *La democratizzazione del rapporto di lavoro*, in *Giornale di diritto del lavoro e delle relazioni industriali*, 1979, 217.

SITZIA A., *Il conrollo (del datore di lavoro) sull'attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso (del lavoratore)*, in *Labour&law Issues*, vol. 2, n. 1, 2016.

SITZIA A., *I controlli a distanza dopo il "Jobs Act" e la raccomandazione R(2015)5 del Consiglio d'Europa*, *Legge e giustizia*, in *il Lavoro nella giurisprudenza*, 7/2015, 671.

SITZIA A., *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali*, Padova, Cedam, 2013.

SOFFIENTINI M., *Protezione dei dati* personali*: nuovo Regolamento Ue*, in *Diritto & Pratica del Lavoro*, 26/2016, 1565.

SORO A., *Liberi e connessi*, Torino, Codice edizioni, 2016.

SORO A., Audizione del Presidente del Garante per la protezione dei dati personali sugli schemi di decreti legislativi attuativi del c.d. Jobs Act presso la Commissione Lavoro della Camera dei Deputati (9 luglio 2015) e la Commissione Lavoro del Senato (14 luglio 2015), in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4119045.

SORO A., Intervento del Presidente del Garante per la protezione dei dati personali, *L'Huffington Post*, 8 settembre 2015, in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/4235378

SPECIALI WIN MAGAZINE, n. 27, *Il manuale dell'hacker 2017*, Edizioni Master, Novembre/Dicembre 2016.

STANCHI A., *Nel Jobs Act il nuovo articolo 4 dello Statuto dei Lavoratori*, in *Guida al Lavoro*, n. 38, 2015, 40.

STANCHI A., *Consultabile la posta elettronica del dipendente sull'e-mail aziendale*, in *Guida al Lavoro*, n. 6, 2016, 41.

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

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

TEA A., *Controlli a distanza:spunti problematici e sviluppi interpretativi*, in *il Lavoro nella giurisprudenza*., 1/2017, 21.

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

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

VALLEBONA A., *Breviario di diritto del lavoro*, sesta edizione, Torino, Giappichelli, 2010.

VIDIRI G., *Controlli datoriali sui dipendenti e tutela della privacy nel nuovo art. 4 Stat. Lav.*, in *Il Corriere giuridico*, 11/2016, 1389.

VIGLIOTTI G. I., *Controlli a distanza e tutela della privacy del lavoratore: la CEDU conferma le scelte del legislatore interno*, in *Massimario di Giurisprudenza del Lavoro*, n. 4, 2016, 209.

ZICCARDI G., *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, in *Labour&Law Issues*, vol. 2, n. 1, 2016.

ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, Raffaello Cortina Editore, 2015.

ZICCARDI G., *Hacker: il richiamo della libertà*, Venezia, Marsilio, 2011.

ZOLI C., *Il controllo a distanza del datore di lavoro: l'art. 4, l. 300/1970 tra attualità ed esigenze di riforma*, in *Rivista Italiana di Diritto del Lavoro*, vol. 1, 2009, 485.

ZOLI C., *Il controllo giudiziario e gli atti di esercizio del potere direttivo: il trasferimento del lavoratore e il mutamento delle mansioni*, in *Diritto delle Relazioni Industriali*, n. 3, 2014, 720.

ZOLI C., *La nuova sicurezza sul lavoro, I Principi comuni*, Commentario diretto da L. MONTUSCHI, Bologna, Zanichelli, 2011.