LUISS Università Guido Carli

Dipartimento

Giurisprudenza

Cattedra

Diritto del lavoro

UTILIZZO DI INTERNET E POSTA ELETTRONICA IN AMBITO AZIENDALE

Relatore
Ch. mo Prof.
R. FABOZZI

Candidata
MICHELA SANTINI
Matr. 109843

ANNO ACCADEMICO

2020 - 2021

Sommario

CAPITOLO III

L'UTILIZZO DI INTERNET IN AMBITO AZIENDALE NELLE PRONUNCE GIURISPRUDENZIALI

UTILIZZO DI INTERNET E POSTA ELETTRONICA IN AMBITO AZIENDALE

Introduzione

L'elaborato affronta un tema di elevata attualità: i limiti relativi all'uso delle mail aziendali da parte del lavoratore dipendente.

La mail, ed internet, costituiscono strumenti divenuti nel tempo indissolubilmente collegati alle attività professionali di molti lavoratori, per cui la consultazione della rete deve considerarsi strumentale allo svolgimento dei propri obblighi.

Ciò premesso, si pone comunque il problema relativo alla necessità di stabilire limitazioni all'accesso alla rete quando esso dovesse inerire esigenze personali, ovvero, quando viene effettuato durante gli orari di lavoro, configurandosi come una sottrazione di tempo alle attività produttive, tra l'altro regolarmente retribuite. I problemi relativi all'abuso dell'impiego della rete, e delle mail, riguardano anche la concessione da parte del lavoratore all'accesso ai computer aziendali ad estranei, esponendo l'azienda a violazione della *privacy*. Dall'altro canto, anche il lavoratore potrebbe eccepire diritti riguardanti la propria *privacy*, per cui ogni ingerenza del datore volta a monitorare l'attività lavorativa, postulerebbe un comportamento illegittimo. Il lavoro che segue analizza ogni aspetto di rilievo, descrivendone le problematiche e le soluzioni adottate non solo dal legislatore ma, altresì, dall'*Authority* per la *privacy* delineando, infine, le pronunce giurisprudenziali sul tema.

L'analisi descritta è stata sviluppata in tre capitoli di cui, il primo, dedicato al potere di controllo attribuito dal legislatore al datore di lavoro. Il tema ha richiesto l'analisi dello Statuto del lavoratore che, all'art.4, ha regolato i controlli a distanza. Inoltre, viene approfondito il

dettato del Regolamento sulla *privacy*, modificato di recente. Il secondo capitolo descrive, nello specifico, la normativa che disciplina gli accessi alla posta elettronica e, quindi alle mail, da parte dei lavoratori, illustrando quanto dettato dal codice civile, dalla direttiva 46/95, dal documento WP29 e dal Testo unico sulla *privacy*.

Infine, il terzo, ed ultimo capitolo, analizza le pronunce giurisprudenziali più note sul tema.

CAPITOLO I

IL POTERE DI CONTROLLO DEL DATORE DI LAVORO

CAPITOLO I

IL POTERE DI CONTROLLO DEL DATORE DI LAVORO

1.1 Considerazioni preliminari

Nel complesso rapporto che si instaura tra datore di lavoro e lavoratore, le funzioni di ciascuno sono state legittimate e limitate dal legislatore, che nel delinearle contempera sia le esigenze produttive dell'imprenditore che gli aspetti relativi alla dignità ed alla privacy[1] del lavoratore.

Il legislatore ha attribuito al datore del lavoro poteri ben specifici: potere strettamente direttivo; potere di vigilanza e sorveglianza e potere disciplinare.

Il primo riguarda l'insieme di poteri che il datore di lavoro può impiegare per indirizzare l'attività d'impresa nella direzione desiderata, mentre il

[1] La più nota accezione di privacy è quella fornita da A. Westin, second cui: "*Privacy is the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place, and circumstances to communicate to others. It means his right to withdraw or to participate as he sees fit. It is also the individual's right tocontrol dissemination of information about himself; it is is own personal possession. Privacy is synonymous with the right to be let alone. Privacy hes also been defined as a "zero-relationship" between two or more persons in the sense that there is no interaction or communication between them, if they so choose. But man lives in community of others, and he also has the need to participate and communicate. When this double-faceted aspect of privacy is coupled with the recognized power of government to function for the public good, there is ample reason for much of the recent concern about invasions and intrusions into individual privacy. A.* WESTIN, *Privacy and Freedom*. New York: Atheneum,1967, p. 7.

potere disciplinare fa riferimento ai contenuti, e alle modalità, degli interventi sanzionatori che è possibile porre in essere nei confronti dei lavoratori. Per quanto riguarda, infine, il potere di vigilanza e sorveglianza, esso inerisce all'insieme di diritti e di limitazioni spettanti al datore nell'ambito del proprio potere organizzativo e direttivo[2]. In merito a tale potere, esso si configura quale interesse legittimo del datore ad adottare forme di 'controllo' sull'operato del lavoratore aventi il fine di verificare l'esattezza dell'adempimento della prestazione, nonché l'uso corretto degli strumenti aziendali che gli sono messi a disposizione per l'espletamento delle mansioni lavorative affidategli.

Nell'esercizio di tale diritto, tuttavia, il datore è sottoposto ad alcuni limiti, essendo sottoposto agli obblighi di rispetto della *dignità* e della *riservatezza* del lavoratore. In tale ottica, pur detenendo il diritto di impedire comportamenti illeciti da parte dei lavoratori, il datore di lavoro non può spiarne la condotta esasperando l'uso dei mezzi tecnologici al punto da sottrarre la dignità e la riservatezza del lavoratore, né gli è concesso di svolgere indagini indiscriminate per risalire alle opinioni politiche, religiose o sindacali del lavoratore. Inoltre, al datore di lavoro sono precluse attività di indagine su fatti che non abbiano rilevanza ai fini della valutazione dell'attitudine professionale e raccolte di dati, se non entro determinati limiti predeterminati, che ineriscano la sfera privata del dipendente. Tali aspetti sono stati disciplinati sia dalle norme

[2] Con la sentenza del n. 6643 del 2012, la Cass. ha confermato il principio secondo cui al fine di distinguere l'esistenza del rapporto di lavoro subordinato da quello autonomo, occorre verificare la sussistenza del vincolo di soggezione del lavoratore al potere direttivo, organizzativo e disciplinare del datore di lavoro, il quale discende dall'emanazione di ordini specifici, oltre che dall'esercizio di una assidua attività di vigilanza e controllo dell'esecuzione delle prestazioni lavorative.

generali contenute nella Costituzione, nel Codice civile e nella CEDU, che dallo Statuto dei Lavoratori e dalla normativa generale sulla *privacy*. Quest'ultima ha di recente subito un'importante integrazione, avvenuta tramite il Regolamento UE 2016/679 (GDPR),cui ha fatto seguito il decreto attuativo n.101 del 10 agosto 2018 che ha sostituito il Codice in materia di protezione dei dati personali e la direttiva 45/96 che precedentemente regolavano la materia[3].

Il capitolo che segue analizzerà gli aspetti descritti nell'ottica di offrire una visione di insieme del tema, evitando di argomentare circa le parti della normativa che riguardano, nello specifico, il controllo della posta elettronica del lavoratore che verranno affrontati nel capitolo successivo.

1.2 Il potere di controllo del datore di lavoro. Il quadro normativo

Le fonti che regolano il potere di controllo del datore di lavoro sono sia internazionali che nazionali.

Il tema della tutela della *privacy* dei lavoratori trova un importante riferimento normativo già nell'art. 12 della Dichiarazione Universale dei Diritti Umani in cui si stabilisce il diritto di ciascun individuo a non essere sottoposto ad interferenze nella propria vita privata, nella casa in cui vive, nella sua famiglia, nella sua corrispondenza, né a subire lesioni del suo onore e della sua reputazione. Tale articolo prevede, dunque, che

[3] M. PERSIANI, *Fondamenti di diritto del lavoro*, Padova, 2015, p.67.

vi sia tutela da parte della legge contro ogni forma di interferenza nella propria vita privata, ovvero contro ogni possibilità di subire lesioni da tale ingerenza. Tale diritto è stato inoltre previsto dall'art.8 della Convenzione per la Protezione dei Diritto dell'Uomo e delle Libertà Fondamentali (CEDU).

Al primo comma dell'art. 8, la Convenzione in oggetto prevede il diritto di ciascun individuo al rispetto della propria vita privata e familiare, nonché del domicilio e della corrispondenza. Al secondo comma dell'articolo è stabilito che '*Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*'.

Il tenore dell'articolo stabilisce, dunque, che l'eventuale compressione di tale diritto, possa essere consentita da parte dell'autorità pubblica solo in casi specifici, riportati dalla stessa norma e caratterizzati dal possedere natura "pubblicistica"[4].

La Carta dei Diritti Fondamentali dell'Unione Europea, sottoscritta a Nizza il 07/12/2000, ha ripreso, all'art. 7, quanto già stabilito dall'art. 8 della CEDU, ovverosia il diritto di ciascuno al rispetto della propria vita privata e familiare mentre, al successivo all'art. 8 provvede a definire il

[4] A. CASTELLANETE, *Notizie e commenti sul diritto interazione e dell'Unione europea*, 299 http://www.marinacastellaneta.it/blog/controllo-delle-mail-aziendali-da-parte-deldatore-di-lavoro-compatibili-con-la-cedu.html.

contenuto del diritto alla protezione dei dati personali, inteso come diritto di ciascun individuo a che i dati che lo riguardano siano trattati secondo il 'principio di lealtà', per finalità determinate, e solo previo consenso della persona interessata. In ogni caso, i dati in oggetto possono essere trattati solo per fondamento legittimo previsto, cioè, dalla legge.

L'articolo prevede, altresì, il diritto di ciascuno ad accedere ai dati raccolti che lo riguardano e di ottenerne la loro rettifica, se necessaria[5].

Le fonti citate non sono, da un punto di vista cronologico, le prime a disciplinare la privacy, ma costituiscono un importante testimonianza del rilievo attribuito al tema. Un primo specifico intervento in materia è evidente già nella Convenzione del Consiglio d'Europa, del 28/01/1981, che mira a garantire ad ogni persona fisica, ed indipendentemente dalla sua cittadinanza o residenza, il rispetto dei diritti e delle libertà fondamentali. La Convenzione in oggetto ha, altresì, dettato i principi riguardanti il diritto alla tutela della vita privata, che emergono in pendenza dell'elaborazione automatizzata dei dati di carattere personale.

Successivamente, con la Raccomandazione R (89) 2 del 18/01/1989 inerente, specificatamente, all'uso dei dati personali 'per fini lavorativi', è stata stabilita la minimizzazione degli eventuali rischi connessi all'uso di metodi di trattamento informatico dei dati degli impiegati.

Anche in questo caso, è stato ribadito il loro diritto, nel preciso ambito lavorativo, al rispetto della vita privata.

La Raccomandazione stabilisce tutti i principi cui attenersi nella raccolta ed utilizzo di dati personali ai fini lavorativi, sia se trattasi di lavoro

[5] F. FABRIS, *Il diritto alla privacy tra passato, presente e futuro*, in *Rivista di scienze della comunicazione*, 2009, n. 2.

espletato in ambito pubblico, che privato. Essi sono stati, successivamente, enunciati dall'art. 12 del Codice della *privacy*[6] .

La successiva Raccomandazione CM/Rec (2015)-5, dell'1/04/2015, nella parte relativa agli artt. (15-21) ha fatto specificatamente riferimento ai rischi sui è sottoposta la *privacy* del lavoratore rispetto all'uso delle nuove tecnologie e mezzi di comunicazione elettronici.

La Comunità Europea è intervenuta in tema di tutela della *privacy* anche con ulteriori misure, di cui la più rilevante è la dir. 95/46/CE del 24/10/1995, che ha ad oggetto il trattamento dei dati personali e la libera circolazione dei dati delle persone fisiche.

Il rilievo della portata di tale Direttiva risiede sia nell'avere fornito la definizione di "dati personali" e di "trattamento", sia nell' avere indicato le modalità con cui le informazioni in oggetto devono essere trattate (ovvero lealmente e lecitamente, nonché per finalità determinate, esplicite e legittime). Con tali presupposti, ai Paesi membri è stato vietato di trattare dati particolari che rivelino l'origine razziale o etnica, le convinzioni religiose o filosofiche e le idee politiche dei soggetti.

Successivamente, sono seguite la dir. 97/66/CE, avente ad oggetto il trattamento dei dati personali nell'ambito delle telecomunicazioni, la dir. 2000/31/CE**,** riportante disposizioni sul mercato elettronico, la dir. 2002/58/CE avente ad oggetto il trattamento dei dati personali e la tutela della vita privata dei lavoratori del settore delle comunicazioni elettroniche e la dir. 2009/136/CE**,** che ha apportato modifiche alla dir.

[6] E. BARRACO, A. SITZIA, *La tutela della privacy nei rapporti di lavoro*, Milano, 2012, p.19.

2002/58/CE. Anche la Costituzione Europea[7], all'art. 67 della parte II, titolo II, stabilisce il diritto alla tutela della riservatezza delle comunicazioni, intesa anche nell'accezione di scambi che avvengono in modalità elettronica, e all'art. 68 indica i principi per il trattamento dei dati personali.

Meritano di essere ricordate anche le "Linee-guida sulla protezione della *privacy* e il flusso transfrontaliero di dati personali", adottate dal Consiglio dell'OCSE nel 2013, che costituiscono un primo aggiornamento della versione pubblicata nel 1980, ed i *Pareri del Gruppo di Lavoro dei Garanti Europei della tutela della privacy* (*Gruppo dell'articolo 29*), tra cui:

- n.8/2001 riguardante il trattamento dei dati personali in ambito lavorativo;
- n. 4/2007 relativo al contenuto dei 'dati personali';
- n. 3/2010 inerente il principio di responsabilità;
- n. 13/2011 riguardante i servizi di geolocalizzazione;
- n. 15/2011 sulla definizione dell'accezione 'consenso';
- n. 3/2015 riguardante la riforma della protezione dei dati.

Si tratta di principi accolti nella normativa interna, di seguito illustrata.

[7] La Costituzione europea, formalmente Trattato che adotta una Costituzione per l'Europa è stato un progetto di revisione dei trattati fondativi dell' UE, redatto nel 2003 dalla Convenzione europea e definitivamente abbandonato nel 2007, a seguito dello stop alle ratifiche imposto dalla vittoria del no ai referendum nei paesi Bassi.

1.2.1. La normativa nazionale

L'ordinamento interno affronta il tema della *privacy*, riferendosi sia direttamente che indirettamente al rapporto di lavoro. Già nella Costituzione italiana è possibile trarre richiami alla tutela della sfera personale delle persone che possono essere ricondotti anche al tema della riservatezza. Nello specifico:

- *l'art. 2 Cost.* riconosce e garantisce i diritti inviolabili dell'uomo, inteso sia nella sua individualità che nelle formazioni di carattere sociale in cui egli interagisce;
- *l'art. 3 Cost.* impone il principio di uguaglianza delle persone;
- *l'art. 15 Cost.* stabilisce il diritto alla inviolabilità della libertà e della segretezza della corrispondenza e di ogni altra forma di comunicazione;
- *l'art. 21 Cost.* enuncia il diritto di manifestare liberamente il proprio pensiero;
- infine, *l'art. 41 Cost.*, nel prevedere la libertà dell'iniziativa economica privata, stabilisce che essa non può comunque svolgersi in contrasto con l'utilità sociale, o in modo da recare danno alla sicurezza, alla libertà e alla dignità umana.

Il tema è ripreso nel Codice Civile che, all'art. 2087 c.c., impone al datore di lavoro di adottare tutte le misure necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro.

Per quanto attiene ai poteri di sorveglianza attribuiti al datore di lavoro, nelle previsioni del Codice Civile rilevano quelli assegnatigli con il fine di garantire il controllo dell'esatta esecuzione della prestazione dedotta in

contratto. Il Codice ha attribuito al datore la possibilità di verificare se il lavoratore usi la diligenza prescritta (art. 2014 c.c., comma 1) e se si attiene alle disposizioni impartitegli (art. 2104 c.c., comma 2[8]).

Anche nel Codice Penale sono state previste tutele a favore del diritto alla riservatezza dei lavoratori.

- gli artt. 614-615 c.p., stabiliscono l'inviolabilità del domicilio, in quanto sfera sottratta alle intromissioni altrui;
- gli artt. 615-*ter*, *quater*, *quinquies* c.p., sono, invece posti a garanzia di "riservatezza informatica" e "domicilio informatico";
- l'art. 615-*bis*, vieta le interferenze illecite nella vita privata;
- gli artt. 616-623-*bis* c.p., stabiliscono l'inviolabilità dei segreti, nonché la tutela della corrispondenza, e delle comunicazioni e conversazioni telefoniche o telegrafiche ovvero attuate con ogni altro mezzo, il segreto professionale, scientifico o industriale e i documenti segreti.
- l'art. 621 c.p. prevede il reato di rivelazione dei contenuti di documenti segreti.

Nel 1996, venne emanata la L. n. 675, in attuazione della Dir. 95/46/CE citata (oggi rivisitata dal Regolamento 2016/679-GDPR) che ha dettato una disciplina generale per la tutela della *privacy* nel trattamento, automatizzato e non, dei dati personali[9]. Ad essa ha fatto seguito il D. Lgs. 30/06/2003, n. 196, noto come 'Codice in materia di protezione dei dati personali' , che raccoglie, in un Testo unico, la L. n. 675/1996 e l'intera normativa, compresi i codici deontologici succedutisi negli anni, in

[8] O. POLICELLA, *Controlli dei dipendenti: gli impianti audiovisivi nel nuovo art. 4 dello Statuto dei lavoratori*, 2015, http:// www.diritto24.ilsole24ore.com.
[9] E. BARRACO, A. SITZIA, *La tutela della privacy nei rapporti di lavoro*, Milano, 2012, p.21.

materia del al trattamento dei dati personali delle persone fisiche e di altri soggetti (anche il TU in oggetto risulta integrato dal Regolamento citato) .

Oltre al riordino della normativa in tema di *privacy*, il Codice si è posto anche l'obiettivo di garantire un livello di tutela della riservatezza più esteso, rispetto a quello stabilito dalla L. n. 675/1996, nonché l'attuazione di una semplificazione degli adempimenti e degli oneri previsti nella disciplina precedente[10].

La maggiore novità del Codice è stata rappresentata dal dispositivo dell'art.1 che riconosce la protezione dei dati personali come autonomo 'diritto della personalità' e, pertanto, avente un proprio contenuto ed una propria disciplina.

Il Codice si compone di tre parti: la prima rimanda alle regole generali, e detta i punti fissi applicabili in tutti i tipi di trattamento di dati;

la seconda concerne le differenti tipologie di trattamento dei dati, soffermandosi, in particolare, su quelle relative all'impiego dei dati personali nell'ambito di una pubblica amministrazione;

la terza parte era relativa alla tutela della *privacy* e stabilisce i casi in cui si ritiene possibile rivolgersi al Garante o al giudice ordinario[11].

Disposizioni ulteriori in materia di disciplina del trattamento dei dati personali sono riscontrabili nel D. Lgs. 10/09/2003, n. 276, in particolare agli artt. 9, 10, 15, 16 e 73, che regolano i flussi di informazioni personali che si realizzano nell'ambito dell'incontro tra domanda ed offerta di lavoro. In tema di limiti al potere di controllo delle attività dei lavoratori,

[10] G. GIUGNI, *Diritto sindacale*, Bari, 2010. A cura di BELLARDI, CURZIO e GAROFOLO, p.70.
[11] C DI MARTINO E F. VOLTAN, *Diritto alla privacy per le imprese ed i professionisti*, 2006, p.112.

la fonte più importante resta lo Statuto dei lavoratori. Il Regolamento 2016/679-GDPR non ha stravolto lo Statuto dei lavoratori se non rispetto ad alcune applicazioni sanzionatorie.

Il diritto alla riservatezza sul luogo di lavoro è rigorosamente previsto dallo Statuto, il cui Titolo I è proprio rubricato *"della libertà e dignità del lavoratore*").

Il Titolo I vieta che il controllo del datore venga esercitato in modo lesivo della dignità e riservatezza del lavoratore. Posto che l'ambito di applicazione dello Statuto dei Lavoratori è limitato al solo rapporto di lavoro subordinato (art. 2094 c.c.), la disciplina dei limiti posti ai poteri di controllo del datore è, a sua volta, circoscritta ai soli artt. da 2 a 6.

Lo Statuto ha riconosciuto, all'art. 1, il diritto dei lavoratori (subordinati) di manifestare liberamente il proprio pensiero nei luoghi di lavoro, senza distinzione di opinioni politiche, sindacali e di fede religiosa, perseguendo il "*proposito ... di contribuire in primo luogo a creare un clima di rispetto della dignità e della libertà umana nei luoghi di lavoro, riconducendo l'esercizio dei poteri direttivo e disciplinare dell'imprenditore nel giusto alveo e cioè in stretta finalizzazione allo svolgimento delle attività produttive*»[12].

L'articolo in oggetto regola, inoltre, varie forme di controllo, in particolare: l'utilizzo delle guardie giurate; gli accertamenti sanitari da parte del datore di lavoro; visite personali di controllo; divieto di indagini sulle opinioni; l'utilizzo del personale di vigilanza; l'utilizzo di impianti audiovisivi e la tutela antidiscriminatoria, sia nell'accezione positiva che negativa.

[12] Senato della Repubblica, V Legislatura, doc. n. 738,2.

1.3 Il personale addetto alla vigilanza

In merito al personale addetto al controllo dei lavoratori, l'art.2 dello Statuto dei lavoratori prevede che il datore di lavoro possa impiegare le guardie particolari giurate[13], soltanto per scopi di tutela del patrimonio aziendale. Ciò postula che le guardie giurate debbano limitarsi a contestare ai lavoratori le sole azioni, o fatti, che attengono alla tutela del patrimonio aziendale e solo in pendenza dello svolgimento dell'attività. È altresì necessario che tale sorveglianza sia dovuta a specifiche e motivate esigenze. In caso di inosservanza, da parte del datore , di quanto disposto, l'Ispettorato del lavoro ne promuove, presso il questore, la sospensione dal servizio, salvo il provvedimento di revoca della licenza da parte del prefetto nei casi più gravi.

La vigilanza dei lavoratori, tra l'altro, non assume una veste di controllo incondizionato, stante il disposto dell'art. 3 dello Statuto, secondo cui '*i nominativi e le mansioni specifiche del personale addetto alla vigilanza dell'attività lavorativa devono essere comunicati ai lavoratori interessati*'.

[13] Di cui agli articoli 133 e seguenti del testo unico approvato con regio decreto 18 giugno 1931, numero 773.

Tale misura mira ad evitare il rischio di controlli occulti e "polizieschi" ai danni dei lavoratori[14]. In merito ai controlli che non ottemperino tali disposizioni, ovverosia che risultino occulti, la giurisprudenza ha chiarito che, ai sensi degli artt. 2086 e 2014 c.c., le norme di cui agli artt. 2 e 3 St. Lav. non escludono il potere dell'imprenditore di controllare direttamente, o tramite la propria organizzazione, oppure ricorrendo a personale esterno all'impresa (come ad esempio imprese di investigazioni) l'adempimento delle prestazioni lavorative. Tali norme ineriscono, piuttosto, l'accertamento, di eventuali mancanze dei dipendenti, già precedentemente riscontrate. In queste evenienze, infatti, si ritiene di essere dinanzi ad una mera ricerca confirmatoria che si sottrae dalle disposizioni inerenti le specifiche modalità in cui si deve effettuare il controllo. L'ipotesi in oggetto riguarda, infatti, contingenze diverse dalla vigilanza dei lavoratori in attività e può realizzarsi legittimamente, anche in modo occulto, senza che vi ostino né il principio di correttezza e buona fede insito nell'esecuzione dei rapporti, né il divieto previsto dall'art. 4 dello stesso Statuto, riferito esclusivamente all'uso di apparecchiature per il controllo a distanza[15].

La giurisprudenza ha anche ritenuto legittimo l'accertamento effettuato dall'imprenditore tramite il ricorso al pedinamento di un lavoratore ad opera di un altro dipendente (il caso riguardava la necessità di stabilire la corretta indicazione del chilometraggio indicato per ricevere un rimborso)[16].

---

[14] A. MINERVINI, *I controlli sul lavoratore e la tutela dell'azienda*, in La giurisprudenza nel lavoro, Milano 4/2014, p.97.

[15] Cass.18/11/2010, n. 23303, in: Il civilista, 2011, 1, 17.

[16] Cass. 10/07/2009, n. 16196, in: Mass. Giust. civ.,2009, 7-8.

Il giudice di merito ha altresì precisato che, alla luce di quanto previsto dagli artt. 2 e 3 St. Lav., l'attività di controllo, posta in essere dal datore che si serve di agenzia investigativa, può essere considerata legittima, solo se il suo ricorso possa ritenersi *proporzionato allo scopo*, nonché assistito da ragioni che possono essere considerate gravi. È stato chiarito inoltre che, in assenza di tali presupposti, gli accertamenti in oggetto dovranno essere considerati inutilizzabili, e l'eventuale licenziamento essere ritenuto illegittimo[17].

1.4 I controlli a distanza ex art. 4 St. Lav.

L'art. 4 dello Statuto dei lavoratori, modificato dall'art. 23, D. Lgs. 14/09/2015, n. 151[18] e successivamente rivisitato dal D. Lgs. n. 185/2016 disciplina il controllo a distanza dei lavoratori. L'art. 4 "ante riforma" stabiliva un generale divieto di uso di impianti audiovisivi e di altre apparecchiature impiegate per finalità di controllo a distanza dell'attività dei lavoratori (comma 1) tuttavia, se tali dispositivi soddisfacevano esigenze organizzative e produttive dell'azienda, oppure se fossero stati strumentali alla gestione della sicurezza sul lavoro (comma 2), potevano ritenersi ammissibili.

In questa ultima ipotesi, se dal loro utilizzo si fosse potuto configurare un'ipotesi di controllo a distanza dei lavoratori, gli impianti in oggetto avrebbero potuto essere installati solo previo accordo con le rappresentanze sindacali o, in mancanza, con la commissione della

[17] Trib. Milano 28/04/2009, in: D.L., 2009, 3, 826.
[18] In attuazione del principio di delega contenuto nell'art. 1, comma 7, L. n. 183/2014.

Direzione Territoriale del lavoro-Servizi ispettivi (DTL) che, in ultima istanza, avrebbe potuto deciderne le modalità d'uso.

Entro trenta giorni dalla comunicazione del provvedimento, il datore, le rappresentanze sindacali aziendali (o, in mancanza, la commissione interna), e i sindacati di cui all'art. 19 dello Statuto dei Lavoratori, avrebbero potuto ricorrere al Ministero del Lavoro e della previdenza sociale contro i provvedimenti assunti dalla DTL - Servizi Ispettivi. In merito, la giurisprudenza ha chiarito più volte che il senso dell'art.4 dello Statuto dei lavoratori vada ricercato nella preservazione della dimensione umana, e ciò richiede di non esasperare l'uso di tecnologie che possano rendere la vigilanza idonea a violare ogni riservatezza nello svolgimento del lavoro[19].

La riforma dello Statuto, avvenuta nel 2015 ad opera del Job Act, D. Lgs. n. 151/2015, nel modificare il comma 2, ha inteso contemperare le due esigenze, quella dei lavoratori con quella del datore di lavoro. Con tale obiettivo, ha preservato le esigenze legate all'organizzazione, produzione e sicurezza del lavoro, ed ha provveduto a delineare una procedura esecutiva.[20]. L'affermazione di principio del nuovo art. 4, comma 1 dello Statuto evidenzia un atteggiamento di apertura del legislatore che, fino ad allora, aveva espresso un palese ed assoluto sfavore nei confronti delle apparecchiature di controllo a distanza.

---

[19] Cass. 17/06/2000, n. 8250, in Not. giur. lav., 2000, 711. Anche in dottrina si veda anche ZOLI C., *Il controllo a distanza del datore di lavoro*: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma, in *Riv. it. dir. lav*., 2009, 04, p.485.

[20] Cass. 17/07/2007, n. 15892, in Guida lav., 2007, 44, 25. Tra l'altro il Trib. Milano 11/04/2005, in *Riv. giur. lav*., 2005, II, 770, ha stabilito che può intendersi per controllo a distanza «sia la supervisione dell'attività lavorativa effettuata in luogo diverso rispetto a quello in cui si trova il lavoratore, sia la registrazione dell'attività lavorativa medesima mediante sistemi di memorizzazione tali da poterne consentire il controllo in un secondo momento.

Il legislatore ha chiarito che, per controllo a distanza devono essere intesi tutti gli utilizzi di strumenti in grado di risalire alla localizzazione ed alla attività del lavoratore, pertanto vi rientrano:

- tessera magnetica marca tempo (*badge*)[21]

- impianti di telecamere a circuito chiuso[22]

- gli apparecchi Kienzle, in grado di stampare schede che permettono di determinare, fra l'altro, l'operatore, il tipo o i tipi di lavorazione, la data, l'ora e il minuto di inizio dell'attività produttiva, la quantità e i ritmi di produzione, i tempi di sosta e la tipologia delle cause di sosta[23];

- sistemi di controllo di entrata e uscita dall'azienda e dal parcheggio aziendale realizzati tramite tessere magnetiche personalizzate, che consentono la registrazione dell'identità del lavoratore e dell'orario in cui si realizza ciascun passaggio[24];

- centralini telefonici automatici in grado di registrare e riprodurre su tabulati la distanza, il tempo, il destinatario ed il numero chiamante per ogni singola telefonata[25] .

- impianti di intercettazione ed ascolto delle conversazioni del lavoratore[26];

- tecnologie biometriche;

---

[21] Trib. Napoli 29/09/2010, in *Riv. it. dir. lav*., 2011, 1, con nota di Fusco; contr. Trib. Napoli 23/09/2010, in *Riv. it. dir. lav*., 1/2011, cit.; ; Trib. Milano 26/03/1994, in *Foro it*., 1994, I, 2894; Trib. Milano 29/09/1990, in *Riv. it. dir. lav*., 1991, II, 550; Pret. Napoli 15/03/1990, in *Not. giur. lav*., 1990, 226.

[22] Cass. 16/07/2000, n. 8250, in *Or. giur. lav*., 2000, I, 613.

[23] Cass. 18/02/1983, n. 1236, cit.; Pret. Milano 04/10/1988, in *Lav. 80*, 1989, 298; Pret. Roma 22/12/1988, in *Foro it.,* 1989, I, 1309; Pret. pen. Milano, 08/02/1986, in *Lav. 80*, 1986, 89; Pret. gen. Milano 21/12/1984, *in Lav. 80*, 1985, 49.

[24] Trib. Milano 09/01/2004, in *D&L Riv. crit. dir. lav*., 2004, 648.

[25] Pret. Milano 04/10/1988, in *Not. giur. lav*., 1989, 436.

[26] Pret. Camerino 24/01/1992, in *Dir. lav.* Marche, 1992, 326.

- ordini di servizio che impongono annotazioni sul giornale dei lavori relative a tutte le operazioni compiute a terminale, che risultano in grado di consentire il raffronto tra i dati forniti dal sistema di elaborazione e quelle normalmente riportati sul giornale dei lavoratori[27] ;

- *computer* palmari, che permettono di conoscere l'attività di ogni lavoratore, nonché di ricostruirne gli spostamenti effettuati sul territorio[28];

- il sistema di controllo statistico di processo c.d. *stat-faes*, che consente di raccogliere dati qualitativi idonei a misurare elettronicamente le varie fasi di lavorazione[29].

- l'istallazione e l'attivazione di apparecchiature volte al controllo degli accessi ("tornelli") agli insediamenti aziendali, con possibilità di registrazione delle ore di entrata e di uscita del personale[30];

- l'installazione di apparecchiature volte ad effettuare un controllo dei costi del servizio telefonico e della loro imputazione contabile al centro di costo nel suo complesso[31].

L'art.23, D. Lgs. n. 151/2015, ha previsto una diversa regolamentazione a seconda che si tratti di: (i) impianti audiovisivi ed altri strumenti ed apparecchiature o di (ii) apparecchi/strumenti dati in uso al lavoratore per svolgere la propria attività, ovvero strumenti di registrazione delle presenze. In linea generale è stato stabilito che l'utilizzo degli impianti

---

[27] Pret. Pisa, 23/06/1992, in *D&L Riv. crit. dir. lav*., 1992, 881.

[28] Nota Min. Lav. 28/11/2006, n. 6585, in *Pratica lav*., 2006,1961, 48.

[29] Pret. Milano, 01/03/1993, in *Or. giur. lav*., 1993, 5.

[30] Pret. Torino 23/01/1992, in *Giur. piem*., 1992, 506.

[31] Nota Min. Lav. 06/06/2006, n. 218, in *Pratica lav*., 2006, 25, 1087.

audiovisivi e di altri strumenti idonei a realizzare controllo a distanza, riceve tutela solo nelle ipotesi in cui esso valga a soddisfare:

- esigenze organizzative e produttive;
- la sicurezza del lavoro;
- la tutela del patrimonio aziendale.

Nell'accezione di 'patrimonio aziendale' rientrano anche i beni cd. immateriali (ad esempio brevetti, programmi *software*, *know how*, etc...).

Il riferimento ai cd. "altri strumenti" ricomprende sia i dispositivi mediante i quali si effettuano delle operazioni, ivi compresa la rilevazione dei dati, sia i programmi *software* che consentono gli accessi Internet ed il monitoraggio della posta elettronica (Cass. 23/02/2010, n. 4375) ed ogni ulteriore tecnologia che consenta un controllo a distanza. In pratica, quando mediante l'applicativo rappresentato, per lo più, da *software,* lo strumento si mostra in grado di svolgere una funzione esclusiva di controllo dell'attività del lavoratore, la regola da applicarsi è quella del primo comma dell'art.4[32] *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*

[32] A. MODESTI, *Il controllo a distanza del lavoratore tra il diritto alla riservatezza e la tutela del patrimonio aziendale*, Roma, *Ragiusan* n. 369/370, 2015, p.104.

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.

La modifica intervenuta nel 2015 ha anche riguardato l'interlocutore a cui le aziende di grosse dimensioni devono rivolgersi per essere autorizzate ad installare gli impianti e/o utilizzare strumenti di controllo, in assenza di accordo sindacale, tali aziende possono ottenere l'autorizzazione dal Ministero del Lavoro[33]. Inoltre, rispetto a prima, in cui l'accordo sindacale o l'autorizzazione della DTL dovevano essere ottenuti per ciascuno stabilimento, con la nuova disciplina è possibile un unico accordo sindacale, ovvero una sola autorizzazione amministrativa del Ministero del Lavoro che sia estendibile a tutte le proprie unità produttive.

Per le aziende di piccole dimensioni, permane l'obbligo di accordarsi con le rappresentanze sindacali aziendali, previa autorizzazione amministrativa preventiva della competente Direzione Territoriale del Lavoro. Un'altra novità[34] introdotta nel 2015 ha riguardato gli strumenti assegnati dall'azienda ai dipendenti ed utilizzati da questi ultimi per rendicontare la prestazione lavorativa e le apparecchiature di

[33] Mentre è stato stabilito che le aziende aventi unità produttive ubicate in province diverse della stessa regione ovvero in più regioni possono stipulare un accordo sindacale con le associazioni sindacali dei lavoratori.

[34] In riferimento alla parte contenuta nell'art. 4, comma 2, dello Statuto dei lavoratori.

registrazione delle presenze (ad es. *tablet*, *smartphone*, *badge*, navigatore satellitare).

In merito a ciò, il nuovo articolo 4 prevede l'assegnazione e l'utilizzo di strumenti di lavoro non essere più considerabile una forma di controllo a distanza, il che li sottrae dagli obblighi di richiesta di autorizzazione. Ora, pertanto, le ragioni del loro impiego divengono fondamentali per l'applicazione di una disciplina piuttosto che dell'altra (Nota Min. Lav. 18/06/2015). La norma prevede che le informazioni raccolte dal datore di lavoro attraverso gli impianti audiovisivi preventivamente autorizzati, nonché attraverso strumenti di lavoro (per i quali non sussistono limitazioni), possono essere utilizzate per "tutti i fini connessi al rapporto di lavoro" e, quindi, anche per quelli disciplinari o per la valutazione del rendimento, purché sia fornita al lavoratore ogni adeguata informazione relativa alle modalità d'uso degli strumenti e di effettuazione dei controlli, e fermo restando il rispetto della normativa in materia di *privacy*. Quest'ultima, è senz'altro la novità più rilevante della riforma dell'articolo. Infatti, una volta fornite tali informative ai propri dipendenti (che riguardano le discipline e le regole aziendali inerenti l'utilizzo delle *e-mail*, degli *smartphone*, dei telefoni cellulari, dei pc, ecc.), gli elementi raccolti tramite tali apparecchiature potranno, ora, essere utilizzati anche in relazione alla valutazione della diligenza del lavoratore. L'art. 4, comma 3, dello Statuto prevede sia l'obbligo di fornire al dipendente un'adeguata informazione relativamente alle modalità di impiego degli strumenti e degli impianti, e sullo svolgimento dei controlli, sia il rispetto da parte dell'azienda delle previsioni di cui al Codice della Privacy (così

come, oggi, integrato dal Reg. 2016/679)[35]. L'assenza di un'esplicita *policy* al riguardo, può determinare una legittima aspettativa del lavoratore, o di terzi, di presupposti di confidenzialità rispetto ad alcune forme di comunicazione[36].

Per tale ragione, i lavoratori sono stati posti nella condizione di conoscere le modalità di controllo del loro operato e i criteri con cui potranno essere utilizzati i dati raccolti per una valutazione disciplinare. In aggiunta, l'ulteriore informativa sulla *privacy*, ha avuto lo scopo di informare il dipendente sul trattamento dei dati personali raccolti tramite i controlli.

Quanto disposto con l'art.4 dello Statuto dei lavoratori trova applicazione anche nel caso in cui le apparecchiature siano state solo installate, senza essere ancora entrate in funzione, ed anche nei casi di controllo discontinuo, perché esercitato in locali in cui i lavoratori possono trovarsi solo saltuariamente[37]. Inoltre, l'applicazione dell'art. 4 è confermata anche laddove il lavoratore sia consapevole del funzionamento di un'apparecchiatura che, pur essendo destinata al solo controllo della produzione consenta, al contempo, di prendere visione della sua attività lavorativa[38].

---

[35]Art. 4, comma 3 St. 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.*

[36] Provvedimento del 30/07/2015, n. 450.

[37] Cass. pen. 15/10/1996, n. 9121, in *Dir. prat. lav*., 1996, 45, 3251; Cass. 06/03/1986, n. 1490, *in Dir. prat. lav*., 1986, 25, 1589; Pret. Milano 04/10/1988, in Lav. 80, 1989, 298; Pret. Roma 13/01/1988, in *Riv. it. dir. lav*., 1988, II, 682; Trib. Catanzaro 26/05/2006, in Guida lav., 2007, 38, 28; Pret. Roma 22/12/1988, in Foro it., 1989, I, 1309.

[38] Cass. 18/02/1983, n. 1236, in *Mass. Giur. lav*., 1983, 143; più recentemente, cfr. Cass. 23/02/2010, n. 4375, in *Guida dir*., 2010, 12, 92.

Sul piano civilistico, l'eventuale violazione dell'art. 4 dello Statuto comporta l'inutilizzabilità del dato informativo così acquisito, escludendo a priori la rilevanza probatoria dei risultati dei controlli dell'attività dei lavoratori, sia a fini disciplinari che risarcitori[39].

La sua violazione integra, inoltre, un illecito penale *ex* art. 38 St. Lav. Al di fuori dei casi legittimanti un controllo, nel caso di violazione dell'art.4 dello Statuto è sempre ravvisabile un'ipotesi di reato (ad esempio, nel caso in cui le apparecchiature di controllo siano state dirette ad evitare furti senza informare i lavoratori). Per contro, non commette reato l'imprenditore che video-sorveglia i lavoratori qualora essi abbiano dato il loro consenso all'unanimità e ciò anche in assenza di un accordo con le rappresentanze sindacali *ex* art. 4, comma 2, dello Statuto[40].

La violazione dell'art. 4 St. Lav., infine, può rilevare anche un caso di condotta antisindacale, *ex* art. 28 dello Statuto[41].

In merito alle pronunce giurisprudenziali, a conferma di quanto in discorso, la Corte di Cassazione[42] ha ritenuto illegittimo il licenziamento di un lavoratore che effettuava telefonate personali durante l'orario di lavoro, rilevate grazie ad un sistema di controllo informatico, introdotto dal datore, senza osservare la procedura di cui all'art. 4 St. Lav. Tali controlli, infatti, ricadono nell'ambito del comma 2 dell'art.4 che, oltre a dovere sottostare alle garanzie procedurali previste, non possono violare

---

[39] Cass. 16/07/2000, n. 8250 in *Lav. prev. Oggi*, 2000, 1694, Cass. 17/07/2007, n. 15892 e Cass. 23/02/2010, n. 4375.

[40] Cass. pen. 11/06/2012, n. 22611, in *Riv. giur. lav*., 2013, II, 876.

[41] Trib. Di Milano 11/04/2005, e Trib. Di Roma 04/06/2005, *in Riv. giur. lav*., 2005, II, 763, con nota di Bellavista; Pret. Cividale del Friuli 04/12/1995, in *Mass. Giur. lav*., 1996, 44; Pret. Roma 22/12/1988, in *Foro it.*, 1989, I, 1309.

[42] Cass. 01/10/2012 n. 16662, in *Foro it*., 2012, 12, I, 3328.

la sfera lavorativa dei singoli prestatori, pertanto i dati in tal modo acquisiti sono inutilizzabili per provare l'inadempimento del lavoratore medesimo.

Le registrazioni raccolte tramite apparecchiature di terzi (es. telecamere di aree esterne al datore di lavoro e gestite da altri soggetti) sono, invece escluse dall'ambito applicativo dell'art.4, essendo, quest'ultimo rivolto al datore di lavoro, ma non a soggetti terzi[43]. Con sentenza del 12/10/2015, n. 20440 la Corte di Cassazione ha stabilito la legittimità del controllo svolto da una società, al di fuori dei locali aziendali, servendosi di guardie giurate o investigatori privati e facendo ricorso a strumenti per la localizzazione e (GPS). Inoltre, con sentenza del 27/05/2015, n. 10995 la Cassazione ha stabilito la legittimità di un falso profilo "Facebook" impiegato per "chattare" con il lavoratore al fine di verificare l'uso dei social durante l'orario di lavoro.

Tale condotta datoriale, ha precisato il giudice, esula dal campo di applicazione dell'art. 4 St. Lav., avendo ad oggetto una decisione assunta dall'azienda a causa della perpetrazione di comportamenti illeciti, idonei a ledere il patrimonio aziendale sotto il profilo del suo regolare funzionamento e della sicurezza degli impianti.

L'art.4 dello Statuto dei lavoratori prevede che la valutazione dello svolgimento della prestazione possa realizzarsi attuando i c.d. "controlli difensivi", ovvero controlli intesi a rilevare mancanze specifiche e/o comportamenti estranei alla normale esecuzione lavorativa, nonché

[43] Cass. 04/04/2012, n. 5371 in *Foro.it*; 2012, 12, I, 3333; Cass. 28/01/2011, in *Foro.it* , 2012,11, II, 345, ovvero installate dalla polizia giudiziaria: ass., 17/05/2013, n. 12091.

illeciti[44]. Parte della giurisprudenza di merito ha precisato che i "controlli difensivi" costituiscano solo una modalità per definire le verifiche finalizzate all'accertamento di condotte illecite del lavoratore, non comportano la raccolta di notizie relative all'attività lavorativa e, dunque, tali controlli non costituiscono una categoria a sé, esentata dall'applicabilità delle previsioni dell'art. 4 St. Lav[45]. Parte della dottrina ha, invece, criticato il suddetto orientamento, vista la difficoltà nel distinguere in concreto l'attività che rientra nella prestazione lavorativa del dipendente da quella che esula da tale prestazione ed ha configurato i "controlli difensivi" non come una modalità ma come riferimento della natura di tali verifiche[46].

L'art. 4 comma 1, terzo periodo, è stato nuovamente novellato dall'art. 5 c. 2, del D. Lgs. n. 185/2016 (in vigore dal 8 ottobre 2016) contente disposizioni correttive ed integrative del D.Lgs. 151/2015. Prima di quest'ultima riforma, unica eccezione al divieto assoluto di utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori, erano rappresentati dai casi in cui

[44] Cass. 12/10/2015 n. 20440, che devono ritenersi fuori dall'ambito di applicazione della norma (cfr. Cass. 03/04/2002, n. 4746, in *Guida lav*., 21, 10, con nota di Nogler, Abuso di telefono aziendale: la decisione su controlli e rimedi e in *Mass. Giur. lav*., 2002, 644, con nota di Bertocchi, e Cass. 10/07/2002, n. 10062, in *Mass. Giur. lav*., 2002, 644.

[45] Trib. Milano 31/03/2004, in *Orient*., 2004, 108, con nota di Cairo, Internet e posta elettronica in azienda: il potere di controllo del datore di lavoro; conf. Trib. Milano 05/07/2006, in *Lav. giur*., 2007, 419; Trib. Teramo 12/05/2006, in *Not. giur. lav*., 2006, 345; Trib. Torino 09/01/2004, in *Giur. piem*., 2004, 131.

[46] A. BELLAVISTA, *Gli accordi sindacali in materia di controlli a distanza sui lavoratori, Il lavoro nella giurisprudenza*, 2014, Milano, p.56.

essi fossero necessari per esigenze organizzative, produttive o di sicurezza del lavoro[47].

Le necessità di riforma avvertite dal legislatore prima nel 2015 e, successivamente nel 2016, sono state motivate dall'avvento dei sistemi di comunicazione mobile, che permettono un collegamento continuo ad *internet* e che, indirettamente, realizzano il monitoraggio dei lavoratori collegati.

Le novità si sono rese necessarie anche in considerazione del fatto che l'evoluzione della tecnologia non consente più la distinzione tra uno strumento di lavoro non idoneo al controllo e lo strumento che lo è, ad esempio nel sistema di rete vi è un *firewall* che consente di includere tutta l'attività svolta sul web. Le modifiche apportate all'art.4 St. Lav. hanno riguardato l'eliminazione del divieto esplicito di controllo a distanza dei lavoratori, individuando le condizioni e le finalità per le quali viene consentito l'utilizzo degli strumenti che comportano tale controllo[48]. Più precisamente, il controllo a distanza è consentito nei soli casi di esigenze di carattere *organizzativo e produttivo, di sicurezza del lavoro e di tutela del patrimonio aziendale*, e non necessita di alcuna autorizzazione. Oggi, dunque, il datore di lavoro può inserire impianti audiovisivi e altri strumenti dai quali derivi anche un controllo a distanza dell'attività dei dipendenti. Tra tali strumenti rientrano, oltre agli impianti di videosorveglianza, *personal computers* fissi e portatili, *tablets* utilizzati senza *password* da più lavoratori, sistemi di geolocalizzazione installati su

[47] In tal caso, era necessario il previo accordo con le rappresentanze sindacali aziendali o, in mancanza, di un'autorizzazione della Direzione Territoriale del Lavoro competente.

[48] M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona".I T – 300/2016, Roma, 2016, p.3.

veicoli utilizzati dai lavoratori, telefoni cellulari utilizzati senza *password* da più lavoratori,centralini telefonici elettronici, registratori di cassa elettronici etc. Come anticipato, tali strumenti possono essere utilizzati dal datore unicamente per esigenze di carattere organizzativo e produttivo, di sicurezza del lavoro e di tutela del patrimonio aziendale. Si badi che si tratta di controllo sull'attività svolta e non del lavoratore ed è solo "incidentale", non potendo assumere i connotati di un monitoraggio costante, nel qual caso si prefigurerebbe una violazione del diritto alla libertà ed alla dignità del lavoratore. La riforma ha confermato l'obbligo di stabilire un accordo sindacale avente ad oggetto le modalità di utilizzo di tali apparecchiature[49]. In mancanza di tale accordo, il datore può richiedere l'autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, alla sede centrale (dell'Ispettorato nazionale del lavoro) in caso di imprese che detengono unità produttive dislocate in ambiti di competenza di più sedi territoriali dell'Ispettorato. Ne discende che, prima di installare ed utilizzare tali sistemi[50] il datore di lavoro deve aver raggiunto un accordo con le rappresentanze sindacali o, quantomeno, aver ricevuto l'autorizzazione pubblica: in entrambi i casi, a tutela di tutti i lavoratori impiegati nell'impresa, è prevista la possibilità di verifica circa la legittimità o la correttezza dell'impiego di tali strumenti.

[49] Accordo stipulato con le RSA o le RSU o se si tratta di imprese con unità produttive ubicate in diverse province della stessa regione o in più regioni con i sindacati comparativamente più rappresentativi sul piano nazionale

[50] Non più i soli impianti audiovisivi come nella versione normativa precedente, ma anche tutti quegli "strumenti dai quali derivi la possibilità di controllare a distanza l'attività dei lavoratori

Il secondo comma dell'art. 4 St. Lav., ha mantenuto il principio della non applicabilità delle limitazioni e delle procedure sopra descritte, nel caso in cui dovessero essere impiegati altri strumenti assegnati ai lavoratori per lo svolgimento della prestazione (ad esempio, telefoni, *tablets*, *computer*,purché assegnati al singolo lavoratore o anche a più lavoratori ma con personalizzazione dell'accesso per ciascuno, *telepass* e carte di credito). Ciò vale anche nel caso delle rilevazioni degli accessi (come ad es. accade nei centri di ricerca, sperimentazione e progettazione) e delle presenze (c.d. lettori *badge*), anche laddove da essi possa potenzialmente derivare la possibilità di un controllo a distanza[51]. La verifica della legittimità del controllo cui si è sottoposti deve avvenire ad opera del lavoratore, che può contestarlo recandosi presso un sindacato, o un legale**.** All'ultimo comma dell'art. 4 è stabilito che il datore di lavoro può utilizzare le informazioni raccolte tramite l'esercizio del potere di controllo a distanza, ovvero con gli strumenti impiegati dal lavoratore per rendere la prestazione, purché i lavoratori siano adeguatamente informati sulle modalità con le quali verrà esercitato il controllo (le informazioni da rendere note riguardano, altresì, i nominativi dei soggetti preposti ai controlli; la periodicità o occasionalità dei controlli; le modalità con cui devono essere utilizzati gli strumenti in dotazione[52]; il tipo di programmi informatici impiegati). Inoltre, devono essere

[51] In tale caso non esiste l'obbligo per il datore di raggiungere alcuna intesa sindacale o di essere autorizzato amministrativamente: il controllo si ritiene libero potendo essere effettuato anche in assenza di un'esigenza organizzativa o produttiva.

[52] I lavoratori devono conoscere se tali strumenti vadano destinati ad un uso privato o lavorativo ovvero promiscuo, e se il loro utilizzo è tollerato o meno dall'impresa.

comunicati gli aspetti relativi alla durata della conservazione dei dati, specificando le informazioni oggetto di temporanea memorizzazione.
Una volta che il datore di lavoro avrà fornito ai propri dipendenti adeguate informazioni circa le regole inerenti l'utilizzo delle e-mail, dei cellulari, dei pc etc., nonché sulle modalità di effettuazione dei controlli aziendali, gli elementi da lui raccolti potranno essere impiegati, anche, con fini disciplinari. Nel caso in cui il datore non avesse adempiuto agli obblighi informativi, invece, i dati raccolti non potranno essere utilizzati a nessun fine, nemmeno a scopo disciplinare. Gli ultimi interventi non hanno apportato modifiche al sistema sanzionatorio previsto dal combinato disposto degli articoli 171 e 172, D.Lgs. n. 196/2003 e dall'art. 38, legge n. 300/1970. In merito a tali novità, il Garante sulla *privacy* ha provveduto ad emanare la *Newsletter* n. 424 del 17 febbraio 2017 con la quale ha ribadito che l'accesso in maniera indiscriminata alla posta elettronica, o ai dati personali contenuti negli *smartphone* in dotazione ai lavoratori, è un comportamento illecito. In pratica, l'Autorità, ha riconosciuto la facoltà del datore di lavoro di verificare l'esatto adempimento della prestazione professionale ed il corretto utilizzo degli strumenti di lavoro, ma ha stabilito che esso deve avvenire nel rispetto della libertà e della dignità dei controllati.

1.5 Perquisizione e controlli e divieto di indagini sulle opinioni

Lo St. dei lav. riserva l'art. 5 alla disciplina sul controllo delle assenze per infermità stabilendo che esso possa essere effettuato solo dai servizi

ispettivi degli istituti previdenziali competenti, che sono tenuti a compierlo quando il datore di lavoro lo richieda. Assegnando ad un ente pubblico i controlli in oggetto, essi non possono, dunque, assurgere a strumenti di vigilanza datoriale[53].

L'art. 6 dello Statuto vieta, invece, le visite personali finalizzate al controllo del lavoratore (vale a dire le perquisizioni personali), ammettendole, unicamente, se indispensabili ai fini della tutela del patrimonio aziendale[54]. Tali controlli possono solo riguardare la qualità degli strumenti di lavoro, o delle materie prime, o dei prodotti (comma 1 art.6) e devono essere effettuati all'uscita dei luoghi di lavoro, salvaguardando la dignità e la riservatezza del lavoratore e adottando sistemi di selezione automatica di gruppi di lavoratori (comma 2, art.6). Per evitare l'uso indiscriminato delle perquisizioni, è previsto che le ipotesi in cui è possibile disporle, e le relative modalità, devono essere preconcordate dal datore di lavoro con le rappresentanze sindacali o, in mancanza, con la commissione interna (comma 3 art.6). Nell'ipotesi in cui non si pervenga ad alcun accordo, su istanza del datore di lavoro, è possibile adire alla Direzione del Lavoro-Servizi Ispettivi, che può emettere un provvedimento impugnabile innanzi al Ministero del lavoro (comma 4, art.6).

La norma in oggetto ha dato origine ad un dibattito interpretativo che ha portato ad interrogarsi circa i limiti sottintesi dall'art. 6, ovvero se i controlli a cui si riferisce riguardino la sola persona fisica del lavoratore o

[53] R. PESSI, *Lezioni di Diritto del lavoro*, Torino, 2012, p.65 ss.
[54] F. SANTONI., *Controlli difensivi e tutela della privacy dei lavoratori*, in *Giur. italiana*, 2016, p.146.

se si estendano anche agli effetti personali e di immediata pertinenza di costui. In merito, la giurisprudenza ha ritenuto che le perquisizioni concernano solo le ispezioni corporali e quegli accessori dell'abbigliamento in che non possono essere considerati diretta ed abituale pertinenza della persona del lavoratore[55]. Per abbigliamento s'intende il vestiario indossato esclusi, secondo il prevalente orientamento giurisprudenziale, "accessori di abbigliamento", cioè, la borsette da donna, borselli da uomo, portafogli e portadocumenti, zainetti. In pratica per questi oggetti personali non è necessario rispettare le condizioni precisate dal citato art. 6, Statuto. Inoltre, esulano dal concetto di perquisizione personale, anche i controlli: sugli oggetti d'arredamento aziendale messi a disposizione del lavoratore, quali armadi, cassettiere e scrivanie negli uffici e armadietti degli spogliatoi; e sull'autovettura del lavoratore, laddove a questi ultimi sia consentito di entrare e/o sostare in aree di proprietà aziendale.

La "visita personale"anche nell'ordinamento processuale, sia civile (artt. 118 e 258 c.p.c.) che penale (art. 309 c.p.p.), è considerata distinta dall'ispezione di cose e luoghi[56], permanendo vietata.

Infine, nel corso del rapporto di lavoro, ed anche ai fini dell'assunzione, l'art. 8 dello Statuto vieta, al datore, di effettuare indagini sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su tutti i fatti che non sono rilevanti ai fini della valutazione della sua attitudine professionale. La violazione dell'art. 8 dello St. lav. comporta il diritto al

[55] Trib. Alba 30/04/2009, in *Giur. Piem*., 2009, 2, 294 e Cons. Stato, sez. VI, 10/10/2002, n. 5439, in *Foro amm*., 2002, 2541.

[56] Tar Milano, (Lombardia), sez. I, 26/06/2014, n. 1657, in *Foro amm*., 2014, 6, 1789 (s.m.).

risarcimento del danno morale, nonché del danno all'immagine e all'identità personale, integrando gli estremi del reato di cui all'art. 38 dello Statuto[57].

1.6 Il trattamento dei dati personali del lavoratore. Il Codice della privacy

Con stretto riferimento all'ambito giuslavoristico, le norme che il Codice della *privacy* detta in materia di lavoro sono limitate alla previsione di un codice deontologico ed alle misure che richiamano la disciplina degli artt. 4 e 8 St. Lav. (che risultano contenute nella Parte I, Titolo VIII, dall'art. 111 all'art.116)[58]. La normativa sulla *privacy* prevede che il datore di lavoro possa procedere al trattamento dei dati personali del lavoratore solo se *strettamente indispensabile* all'esecuzione del rapporto di lavoro. Pertanto, le informazioni che possono essere trattate sono relative ai soli dati riguardanti l'attività lavorativa e ad alcuni dati relativi alla sfera personale, come ad esempio quelli riguardanti la residenza, i recapiti telefonici e le informazioni sul nucleo familiare. Nella bacheca aziendale possono essere liberamente affissi turni lavorativi o feriali ed ordini di servizio, ma è vietato pubblicare notizie relative alle retribuzioni percepite dai lavoratori, alle sanzioni disciplinari cui sono stati sottoposti e all'eventuale adesione a sindacati.

[57] Trib. Milano 11/08/2006, in *D.L. Riv. crit. dir. lav.*, 2006, 4, 1129 (s.m.), con nota di Bonsignorio.

[58] Oltre a queste vi sono disposizioni in tema di lavoro domestico che si limitano a garantire la privacy del datore di lavoro e, in tema di telelavoro, con previsione estremamente generica, il rispetto della personalità e della libertà morale del lavoratore.

Inoltre, non è consentito rendere pubbliche notizie dalle quali sia possibile desumere lo stato di malattia o l'esistenza di patologie del lavoratore.

Le Pubbliche Amministrazioni possono pubblicare sui propri siti *web* istituzionali documenti contenenti dati personali solo se la normativa di settore lo preveda espressamente. I dati sanitari dei lavoratori devono essere conservati in fascicoli separati ed il datore non può accedere alle cartelle cliniche dei lavoratori sottoposti ad accertamenti dal medico del lavoro. Nell'eventualità si profilino presupposti per la denuncia di infortuni o malattie professionali all'Inail, il datore deve limitarsi a comunicare unicamente le informazioni che riguardano la patologia denunciata, evitando ogni altra pubblicizzazione di dati. L'utilizzo dei dati biometrici[59] è vietato, ad eccezione dei casi in cui tali dati si rendano necessari per il presidio agli accessi ad aree sensibili, oppure per consentire l'utilizzo di macchinari pericolosi, riservato ai soli soggetti qualificati. Le impronte digitali e l'emissione vocale possono, inoltre, essere utilizzate per l'autenticazione informatica (accesso a banche dati o a PC aziendali) e per la firma grafometrica, prevista per la sottoscrizione di documenti informatici. In alcuni casi, individuati dal Garante della *privacy*, il datore di lavoro non è tenuto a richiedere il consenso al personale per adottare tecnologie biometriche ma deve, comunque, informare i dipendenti sui loro diritti, sugli scopi e sulle modalità del trattamento dei loro dati.

[59] Come ad esempio delle impronte digitali.

In linea generale, la liceità del sistema di rilevazione deve essere valutata sul piano della conformità ai principi di *necessità, proporzionalità, finalità e correttezza* (artt. 3 e 11 del Codice).

Il datore di lavoro può predisporre controlli giustificati da motivi organizzativi o di sicurezza solo se di pertinenza e non eccessivi.

Il nuovo Regolamento europeo sulla *privacy* (GDPR), entrato in vigore il 19 settembre 2018, tramite il D.Lgs n.101, ha apportato diverse novità al vecchio Codice ed ha stabilito che, per il trattamento dei dati sensibili il consenso deve essere sempre esplicito, non essendo tuttavia necessario che sia redatto in forma scritta.

In generale, le nuove disposizioni prevedono misure più stringenti per i titolari delle aziende riguardo il trattamento dei dati personali in possesso, in particolare rispetto alla loro "comunicazione" e "diffusione"[60]. Di seguito l'analisi delle principali novità apportate dal Regolamento.

1.6.1 L'adeguamento al Regolamento 2016/679: il Decreto n.101/2018

Le novità del GDPR in ambito giuslavoristico hanno riguardato alcune integrazioni agli articoli 111-116 del Codice sulla *privacy*[61].

[60] Pertanto, per il mancato rispetto delle regole saranno applicate sanzioni amministrative.

[61] Il D. Lgs n.101 del 2018 ha abrogato il precedente art. 11 del Codice della *privacy* che riportava:
1. I dati personali oggetto di trattamento sono:
A) trattati in modo lecito e secondo correttezza;
B) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
C) esatti e, se necessario, aggiornati;

Il nuovo art. art. 111 (Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro) stabilisce, ora, che: '*Il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato*'.

L'art.88 in commento stabilisce che i Paesi membri possono prevedere, anche utilizzando lo strumento dei contratti collettivi, norme volte alla tutela del trattamento dei dati dei dipendenti per finalità di assunzione, ovvero di esecuzione del lavoro, di gestione, organizzazione e pianificazione, parità di trattamento, sicurezza, difesa del diritto di proprietà del datore, nonché per motivi di cessazione del rapporto di lavoro. L'articolo raccomanda ai Paesi membri di adottare misure per la salvaguardia della dignità, degli interessi legittimi e dei diritti fondamentali degli interessati.

Inoltre, si raccomanda di estendere la protezione dei dati anche in pendenza del trasferimento di dati nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese. Novità hanno riguardato, anche, l'art. 111-bis (Informazioni in caso di ricezione di *curriculum*), che

---

D) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

E) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

prevedendo che *'Le informazioni di cui all'articolo 13 del Regolamento*[62]*, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all'invio del curriculum medesimo. Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento, il*

[62]Articolo 13 Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato 1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili. 2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo;
e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2. 4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

consenso al trattamento dei dati personali presenti nei curricula non è dovuto'. Anche l'art.113 ha subito delle modifiche[63] e, rispetto al dispositivo precedente è stato aggiunto il rimando all'art.10 del d.lgs 276, che prevede il *'Divieto di indagini sulle opinioni e trattamenti discriminatori'*.

Il nuovo tenore dell'articolo è, ora il seguente: *'E' fatto divieto alle agenzie per il lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonche' ad eventuali controversie con i precedenti datori di lavoro, a meno che non si tratti di caratteristiche che incidono sulle modalità di svolgimento della attività lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attività lavorativa. E' altresì fatto divieto di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo'*. Il Regolamento n. 2016/679[64]esorta l'intervento per favorire la trasparenza del trattamento, il trasferimento di dati personali all'interno delle unità produttive o di un gruppo di imprese che svolge una comune attività e l'adozione di sistemi

[63] Venendo articolato, nel modo seguente, '*Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n.300 nonché dall'articolo 10 del decreto legislativo 10 settembre 2003, n. 276'*.

[64] Il Regolamento invita gli Stati ad intervenire in vari ambiti, tra cui l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, la gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.

di monitoraggio sul posto di lavoro. Il Decreto di adeguamento del regolamento (D. Lgs. n. 101 del 10 agosto 2018) ha confermato il rilievo degli artt. 1, 4 e 8 dello Statuto dei lavoratori (L. n. 300/1970) e l'interpretazione del Gruppo di lavoro art. 29 (W29) in cui si stabilisce che ogni lavoratore, indipendentemente dal tipo di contratto a lui applicato, ha diritto al rispetto della vita privata, della sua libertà e dignità. Inoltre, viene assodato quanto già deciso nel Codice della privacy che ciascun lavoratore debba essere informato circa le modalità di trattamento dei dati personali.

Come anticipato, il decreto ha dato conferma anche di quanto stabilito dal Gruppo di lavoro art.29 in merito all'adozione di misure preventive volte alla protezione della riservatezza dei lavoratori redigendo, se del caso, anche una valutazione precisa dell'impatto generale del trattamento, avendo cura di rilevare i dati in modo da contemperare sia quanto necessario per il legittimo interesse aziendale, sia quanto ammesso dall'uso delle nuove tecnologie informatiche (*principio del bilanciamento*). Il decreto di adeguamento[65] prevede che nel trattamento dei dati personali i datori devono tenere ben presenti i diritti fondamentali dei lavoratori, tra cui, *in primis*, il diritto alla loro riservatezza.

Per quanto riguarda le basi giuridiche del trattamento dei dati, esse dovranno rinvenirsi: *nell'adempimento di obbligazioni previste dalla legge; nell'esecuzione di obblighi derivanti da un contratto di lavoro; nell'interesse legittimo del datore*.

[65] Che è rivolto sia ai lavoratori dipendenti sia a quelli autonomi, indipendentemente dalla stipula o meno di un contratto di lavoro subordinato.

Il WP29 esclude dalle basi giuridiche del trattamento dei dati dei lavoratori il consenso di questi ultimi in quanto,poiché considerando il tipo di rapporto di soggezione nei confronti del datore, esso non potrebbe mai ritenersi prestato liberamente.

L'interesse legittimo del datore di lavoro, necessita di proporzionalità del trattamento dei dati per il perseguimento di una finalità legittima. Inoltre è necessario adottare tutte le misure di sicurezza utili per bilanciare la finalità del trattamento con i diritti e le libertà fondamentali dei lavoratori. L'art.35 del Regolamento - GDPR prevede l'eventuale compilazione del c.d. DPIA, ovvero di una valutazione di impatto del trattamento. Il datore di lavoro è tenuto anche ad adottare specifiche misure di sicurezz**a** per prevenire violazioni della riservatezza degli interessati, tra cui:

- il divieto di monitoraggio delle cartelle/dei file e/o delle comunicazioni personali dei dipendenti;
- l'esclusione delle cd. "aree sensibili" dalle zone sottoposte a monitoraggio;
- la previsione di un monitoraggio "a campione", rispetto ad una sorveglianza continuata nel tempo[66].

Il datore di lavoro è comunque tenuto a garantire agli interessati il diritto di opporsi al trattamento dei propri dati, diritto loro conferito dall'art. 21 del GDPR. I dati possono essere "*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al*

[66] Sul punto, per l'Italia, cfr. Prov. Garante Privacy n. 247/2017 in: *www.garanteprivacy.it*.

conseguimento delle finalità per le quali sono trattati" (art. 5, c. 1, lett. e GDPR). Inoltre, in alcuni casi il periodo di conservazione deriva da limiti normativi[67]. Con il parere espresso dal gruppo, WP29 sono stati individuati 9 scenari tipici di trattamento di dati personali dei lavoratori e, per ciascuno di essi, il datore è tenuto a procedere alla previa individuazione della base giuridica del trattamento, nonché a verificare l'effettiva necessità delle attività di trattamento e alla valutazione della correttezza, ma anche alla proporzionalità rispetto alle finalità che vengono perseguite. Nella fase di assunzione, il datore può trattare i dati dei potenziali candidati presenti sui loro profili social (opinioni personali, interessi, ecc.) nei soli casi che prevedono il loro impiego per finalità lavorative. È altresì necessario che tali dati personali siano ritenuti necessari e rilevanti per la prestazione lavorativa richiesta. In ogni caso, il datore è tenuto ad informare il candidato del trattamento dei suoi dati personali[68]. Per il trattamento dei dati dei lavoratori presenti sui social, il datore deve attenersi agli stessi presupposti stabiliti per il trattamento dei dati dei candidati tradizionali: *informativa preventiva del trattamento resa agli interessati, esistenza del presupposto della necessità del trattamento rispetto all'interesse perseguit*o[69]. Per quanto attiene al monitoraggio dei dati ottenuti dalla strumentazione informatica dei lavoratori,[70] si incoraggiano i datori ad adottare soluzioni volte a prevenire il ricorso ad

[67] Es. i dati necessari per la tenuta del libro unico del lavoro possono essere conservati per cinque dalla data dell'ultima registrazione *ex* art. 6 D.M. 9 luglio 2008.

[68] Mediante, ad esempio, l'inserimento di una specifica indicazione all'interno dell'annuncio di lavoro.

[69] A tal riguardo, si impone sul datore di lavoro l'onere di provare anche l'insussistenza di strumenti meno invasivi per il raggiungimento delle finalità del trattamento.

[70] Informatica (es.: e-mail ricevute/inviate; siti web visitati; telefonate effettuate).

accessi "successivi" a tali informazioni (ad esempio, quelli presenti nella cronologia web e/o nella casella di posta elettronica).

Per consentire ai lavoratori di servirsi degli strumenti informatici in modalità legittima, il datore deve preventivamente informarli circa i limiti dell'utilizzo dei dispositivi. Tra le soluzioni consigliate dal gruppo WP29 rientra l'informativa circa l'elenco di siti in cui la navigazione è vietata; la previsione di calendari in cui accedere alla posta personale; l'ufficializzazione di una policy aziendale per l'uso della strumentazione informatica. Al pari di quanto previsto dal Codice della privacy, anche il Regolamento ha disciplinato il trattamento dei dati sensibili e, in particolare, di quelli biometrici dei lavoratori. Ai sensi dell'art. 9 del GDPR[71] fornire ai lavoratori specifici dispositivi indossabili che monitorino lo stato di salute[72]sia nelle ore di lavoro che al di fuori e trattare i dati così rilevati, è da considerarsi illecito[73].

Tra gli esempi di tali strumenti si pensi all'installazione di un sistema di rilevazione dei dati biometrici dei dipendenti, che mira al monitoraggio dell'accesso ad aree in cui persistono informazioni riservate ma che è, al contempo, in grado di consentire al datore di controllare lo svolgimento della prestazione lavorativa. In questi casi esiste un legittimo interesse del titolare al monitoraggio, consistente nella tutela di informazioni riservate di natura aziendale. Sebbene consentito, tuttavia occorrerà anticipatamente rendere un' idonea informativa ai lavoratori. L'utilizzo

[71] Ex 8 della Direttiva 95/46/CE.

[72] Numero dei passi, battiti cardiaci e ore di riposo notturno.

[73] I dati personali raccolti tramite tali strumenti, pertanto, possono essere trattati solo dai diretti interessati ed eventualmente dal fornitore del servizio.

delle tecnologie che consentono il video monitoraggio dei lavoratori [74]è illecito, essendo considerato sproporzionato rispetto alla tutela dei diritti e delle libertà fondamentali degli interessati. Per valutare la liceità del trattamento dei dati riguardanti la localizzazione dei lavoratori, mediante installazione di impianti GPS sui veicoli aziendali affidati, il regolamento distingue due casi: si riterrà illecito qualora il trattamento in oggetto venga posto in essere con l'unico fine di controllare il comportamento dei dipendenti e/o la loro collocazione geografica[75]; mentre, laddove tale monitoraggio viene effettuato con il fine del perseguimento di scopi legittimi, quali la tutela della sicurezza dei veicoli e/o dei lavoratori ovvero, ancora, per la pianificazione in tempo reale di alcune attività lavorative, esso è da considerarsi lecito[76].

Tuttavia, si suggerisce di inserire all'interno di ciascun veicolo un' 'informativa privacy' in cui si dichiara l'avvenuta installazione del GPS.

Laddove i lavoratori sono autorizzati ad utilizzare le auto anche per finalità private, si suggerisce di garantire ai lavoratori la possibilità di disattivare il sistema GPS.

Infine per ciò che attiene al trasferimento dei dati personali, l'art.17 GDPR lo consente se indirizzato ai clienti finali ma solo se esiste un legittimo interesse del titolare. Se, invece, tali dati vengono comunicati tra società afferenti il gruppo cui fa parte l'impresa che ha sede fuori dall'Italia, ciò è legittimo dietro garanzia di un adeguato livello di protezione dei dati da

[74] Ad es.: monitoraggio dell'espressione facciale mediante la videocamera dello *smartphone* affidato ai lavoratori.

[75] Ciò è anche ribadito in: WP29 Parere n. 13/2011,in: *www.garanteprivacy.it*

[76] Sul punto anche WP29 parere n. 5/2005, in: *www.garanteprivacy.it*.

parte dello Stato estero e, ove mancante, occorre una apposita deroga[77]. È possibile trasferire anche le valutazioni sul lavoratore, tratte da tali dati, ma solo se queste costituiscono mere elaborazioni di dati oggettivi.

1.7 La videosorveglianza sul luogo di lavoro: tra potere di controllo del datore e tutela della *privacy* dei lavoratori

Stante il principio che vieta l'utilizzo arbitrario di strumenti di controllo, come la videosorveglianza o la geo-localizzazione, il datore di lavoro non può, in via generale, controllare a distanza dei lavoratori[78].

Come si è visto, prima della riforma intervenuta prima nel 2015 e poi nel 2016,l'art.4. della Legge n.300/70 stabiliva che gli impianti e le apparecchiature utilizzabili, anche per il controllo a distanza dell'attività dei lavoratori, avrebbero potuto essere installati previo accordo con i sindacati aziendali, oppure, in mancanza di questi ultimi, con la commissione interna.

In particolare, tali dispositivi non avrebbero potuto essere utilizzati per verificare l'osservanza dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa. Si è detto che, l'articolo 4 dello St. Lav. è stato riformato dall'art. 23 del D. Lgs. n. 151/2015, in vigore dal 24 settembre 2015, attuativo del c.d. "Jobs Act", ovvero legge delega n. 183/2014, art. 1, comma 7, lett. f). L'art.23 in oggetto reca

[77] Richiamando i principi generali per il trasferimento dei dati previsti dalla Direttiva 95/46/CE e, attualmente, trasposti all'interno del GDPR.

[78] D'ARCANGELO L., *I controlli a distanza dopo il Jobs Act. Dallo Statuto dei lavoratori alla disciplina sulla protezione dei dati personali*, in *Mass. di Giurisprudenza del Lavoro*, n. 10, 2016, p.9.

la: «*revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore*», ed ha introdotto importanti modifiche rispetto alla possibilità del datore di lavoro di operare un controllo sull'attività lavorativa svolta dai propri dipendenti.

In merito al tema della videosorveglianza, la nota dell'Ispettorato Nazionale del Lavoro n. 4619 del 24 maggio 2017 ha provveduto a fornire alcuni ulteriori chiarimenti. La procedura autorizzativa dell'Ispettorato territoriale del Lavoro, successiva al mancato accordo con gli organismi sindacali interni, può essere sostituita da un accordo sindacale poiché, anche laddove sia stato rilasciato il provvedimento autorizzatorio, in seguito a mancato accordo sindacale, l'autorizzazione in oggetto può, comunque, essere sempre sostituita da un successivo accordo. Si ricorda, infine, che le organizzazioni sindacali deputate al raggiungimento dell'accordo sono la RSU o la RSA e tutti i soggetti coinvolti nella contrattazione c.d. di prossimità ex art. 8, D.L. n. 138/2011[79].

Sebbene si sia cercato di analizzare l'intero *corpus* normativo riguardante la vigilanza dei lavoratori, è stata omessa la disciplina relativa agli aspetti

[79] Ovvero le associazioni dei lavoratori comparativamente più rappresentative sul piano nazionale o territoriale per la sottoscrizione di contratti a livello aziendale o territoriale.
Tale articolo trova applicazione solo in presenza di determinate finalità, fra le quali la "maggiore occupazione, la qualità dei contratti di lavoro, l'adozione di forme di partecipazione dei lavoratori, l'emersione del lavoro irregolare, gli incrementi di competitività e di salario (ecc.)"

inerenti i controlli sulla posta elettronica, seppure disciplinati nelle fonti analizzate. Il capitolo che segue, approfondirà tale tema.

CAPITOLO II
IL CONTROLLO DEL TRAFFICO TELEMATICO AZIENDALE. ASPETTI NORMATIVI

CAPITOLO II

IL CONTROLLO DEL TRAFFICO TELEMATICO AZIENDALE. ASPETTI NORMATIVI

2.1 Il traffico telematico, l'analisi della questione: tra difesa del patrimonio aziendale e tutela della *privacy*

Come ampiamente illustrato nelle pagine precedenti, le aziende attuano controlli per vari motivi, essenzialmente legati alla necessità di garantire che il lavoro si svolga secondo criteri precisi ma, anche, per tutelare l' impresa stessa ed il suo patrimonio. Il controllo dei lavoratori può consentire, però, di acquisire dati ed informazioni che esulano dagli obiettivi descritti, in tale ottica il legislatore non consente, in nessun caso, che il monitoraggio dei lavoratori si trasformi si trasformi in arbitrario esercizio di potere. Il Gruppo di lavoro sulla protezione dei dati Articolo 29 (WP29) ritiene che "*i dati vanno raccolti per uno scopo determinato, esplicito e legittimo, evitando di trattarli in un secondo momento in modo incompatibile con tali finalità*[80]."

Come si vedrà in seguito, l'operatività di tale esimente è subordinata alla conoscibilità della finalità del controllo, che pertanto dovrà opportunamente essere resa pubblica dall'imprenditore nella esplicitazione della sua policy aziendale.

[80] "*Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro*", adottato il 29.05.2002

Oggigiorno, lo strumento di lavoro più diffuso e accessibile è il computer, spesso inserito in una rete aziendale (LAN), ed avente la predisposizione alla connessione alla rete Internet. Il computer è al contempo strumento di lavoro e dispositivo utile per soddisfare esigenze personali del lavoratore, quali la navigazione in rete o l'accesso alla propria posta elettronica. Rileva osservare che, il dipendente che si distrae con la navigazione in Internet per fini extra lavorativi, o che scrive, o legge, mail personali sottrae tempo (retribuito) e produce rallentamenti al processo produttivo. Il caso descritto trova una disciplina nell'art.2104 c.c. che imponendo al lavoratore l'obbligo di diligenza nella prestazione lavorativa, sanziona gli eventuali usi personali dei beni aziendali affidatigli per l'espletamento delle mansioni assegnate.

La fattispecie è stata interpretata in maniera completamente opposta dal Gruppo – Articolo 29 (WP29), che consiglia di concedere gli strumenti informatici anche per usi personali. La posizione della dottrina più attenta è stata quella di affrontare tali aspetti da più angolazioni, giungendo ad escludere che il mero utilizzo della connessione ad Internet da parte del lavoratore possa ritenersi fattispecie di reato ma riconoscendo che l'uso improprio degli strumenti informatici costituisca un viatico per la diminuzione della capacità di memoria e di larghezza di banda disponibile arrecando, dunque, un danno oggettivo[81].

Ad acuire le criticità di un siffatto uso privato del computer si aggiunge la necessità di tutelare il patrimonio aziendale ai fini della "sicurezza

[81] L.M. DE GRAZIA, *In Internet ed Intranet, sicurezza e privacy: i pericoli nascosti nell'applicazione della l. 675/96 e del d.lgs. 318/99* in: "*Furto di identità ovvero frode da impersonificazione: Cosa è? Quali sono i rischi? quanto è diffuso? come difendersi*?", 2013, in *www. Europeanprivacycentre.eu.*

informatica", il che comporta la necessità di proteggere le informazioni e i dati aziendali da possibili attacchi provenienti dall'esterno.

Tali danneggiamenti ai sistemi informatici sono agevolati dalla negligenza del dipendente che, in assenza di prescrizioni, potrebbe arrivare ad installare programmi lesivi per il sistema informatico, comunicare *password*, introdurre virus rispondendo ad attacchi mirati ecc.. Non minore è il rischio di danni alla reputazione a cui si espone un'azienda dai cui indirizzi mail partono messaggi dal dubbio decoro.

Alla luce di quanto descritto, il controllo del datore di lavoro non necessita unicamente di essere volto a rilevare eventuali rischi informatici dovendo anche, perseguire la tutela delle condizioni di lavoro imposte dalla legge. In particolare, il tenore dell'art.2087c.c., rinvia all'obbligo generale di sicurezza cui l'imprenditore deve attenersi[82].

Si tratta di una norma la cui inosservanza determina casi di responsabilità civile, pertanto il controllo degli accessi ad Internet e delle e-mail entranti, si configura addirittura come un obbligo per il datore di lavoro tenuto a prevenire eventuali lesioni a carico del lavoratore.

Se si pensa allo scambio di e-mail tra dipendenti, aventi ad oggetto offese, maldicenze o battute si configura, inoltre, un'ipotesi di responsabilità che il datore di lavoro è tenuto a prevenire non più nell'ottica di garantire sicurezza ma in quella di porre in essere ogni misura per impedire il *mobbing*. Inoltre, anche il D. Lgs. n. 626 del 1994 ha posto obblighi precisi a carico del datore, imponendogli la predisposizione di misure

[82] La norma testualmente dispone che: "l'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro".

preventive di sicurezza, nonché di provvedere alla formazione dei lavoratori, all'organizzazione di servizi di prevenzione e di protezione e ad istituire un rappresentante dei lavoratori in funzione di garante dell'applicazione delle norme a tutela della salute e della sicurezza.

In linea con tali obiettivi, rispetto all'uso del computer è previsto che il dipendente abbia "*una pausa di quindici minuti ogni centoventi minuti di applicazione continuativa al videoterminale*"[83]. Un dispositivo di segnalazione del tempo trascorso dal dipendente al computer sarebbe, dunque, in perfetta coerenza con la normativa dettata in tema di sicurezza, ma, si potrebbe osservare, si tratta pur sempre di uno strumento di controllo dei lavoratori[84].

Ciò evidenzia che, anche quando la finalità del controllo è posta a tutela del lavoratore, il datore di lavoro è in grado di reindirizzarla alla verifica dell'adempimento della prestazione lavorativa.

Un' ulteriore perplessità sopraggiunge dalla necessità di contemperare le due esigenze (di sicurezza del lavoratore e di sicurezza del patrimonio aziendale), ovvero resta da rilevare l'esposizione al rischio del datore di lavoro, nel caso di gestione irresponsabile degli strumenti telematici.

L'abuso da parte dei dipendenti degli strumenti informatici espone il datore al rischio di un coinvolgimento civile, e penale, nel caso vengano perpretati di illeciti nei confronti di terzi.

Il primo profilo di responsabilità (resp. civile) deriva dall'obbligo risarcitorio connesso alla commissione di un reato o di un fatto illecito da

---

[83] D.Lgs. 626/94. Titolo VI – Uso di attrezzature munite di videoterminali, 'art. 54.

[84] S. SUTTI, *La sicurezza dei sistemi informativi aziendali, norme protettive, oneri e misure obbligatorie, in La privacy in Internet*, a cura di A. LISI, Ed. Simone, 2003, p111.

parte del dipendente, infatti, l'art. 2049 c.c. stabilisce che "*i padroni e i committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze a cui sono adibiti*". In questo caso, il terzo danneggiato può chiedere il risarcimento del danno subito, sia a colui che ha commesso direttamente il fatto (il dipendente), sia al datore.

Da un punto di vista penale, sebbene trattasi di responsabilità personale, il nostro ordinamento prevede la categoria dei cosiddetti "reati omissivi impropri" che si basa sul dispositivo dell'art. 40 c.p. che stabilisce che "*Nessuno può essere punito per un fatto preveduto dalla legge come reato, se l'evento dannoso o pericoloso, da cui dipende la esistenza del reato, non è conseguenza della sua azione od omissione*".Tali reati si concretizzano nella violazione di un generico obbligo giuridico di impedire determinati eventi dannosi per cui, penalmente, in caso di illecito imputabile al lavoratore, sarà perseguibile anche il datore di lavoro per non aver impedito l'azione tramite l'adozione di idonee misure di prevenzione e controllo[85].

Nelle grandi aziende, l'estensione della responsabilità penale sarebbe esclusa qualora il titolare (o gli amministratori) decidano di delegare la funzione di prevenzione e controllo ad un altro soggetto. Perché ciò sia valido sono richieste alcune condizioni: la delega deve essere scritta e accettata dal delegato; il delegato deve essere tecnicamente competente, qualificato e idoneo allo svolgimento del compito; il delegato deve avere una piena autonomia decisionale e organizzativa, e dotato delle risorse

[85] A titolo di concorso nel reato.

necessarie per espletarla; il delegante non deve interferire nei compiti assegnati al delegato[86]. Relativamente all'uso telematico, in presenza delle suddette condizioni il coinvolgimento penale dell'azienda risulterà essere circoscritto alla sola figura che effettivamente ha il controllo sul traffico dei dati[87].

La dottrina opera una distinzione tra reati commessi 'mediante Internet' e reati commessi 'su Internet', inerendo i primi, ai reati comuni, previsti nel Codice Penale o da altre leggi speciali ed i secondi ai reati di nuova previsione, introdotti con la legge n.547 del 1993 in tema di criminalità informatica.

I reati commessi 'mediante Internet' riguardano fattispecie eterogenee, previste ben prima della apparizione della 'rete', quali i delitti legati alla parola, in particolare l'ingiuria[88], l'onore e la diffamazione[89]; l'istigazione a delinquere, fino all'apologia[90] e, infine, la rivelazione di segreti professionali o industriali[91].

Inoltre è possibile riconoscere profili di rilevanza penale nello *spamming*, ovvero nell'invio, talvolta in modo continuativo, di messaggi non richiesti[92] (lo *spamming* si configurerebbe anche nella fattispecie di 'molestia' o 'disturbo' alle persone, prevista dall'art.660 c.p.), oppure in

---

[86] F.S. FORTUNA, *I reati in materia di lavoro, Trattato di diritto penale dell'impresa*, vol. VIII, CEDAM, 2002. In giurisprudenza ex multis Cass. Pen., Sez. IV, 22.03.1985 in *Giust. Pen.*, 1986, II, p. 70.

[87] Incidentalmente, vista la similarità delle competenze richieste, si suggerisce che tale ruolo potrebbe essere rivestito da una delle figure create dalla normativa sulla *privacy*; ad esempio il responsabile del trattamento.

[88] Art. 594 c.p.

[89] Art.595 c.p.

[90] Art. 414 c.p. e Artt. 266, 272, 327 c.p..

[91] Artt. 622, 623 c.p.

[92] M. DE GIORGI, *La tutela della privacy per il consumatore in rete, in La privacy in Internet*, a cura di A. LISI, Ed. Simone, 2003, p.88.

quella di trattamento illecito di dati personali disciplinato dall'art. 167 del Testo Unico sulla Privacy[93].

Profili di reati penali si rinvengono, anche, nelle ipotesi di impiego, a nome proprio, di documenti scritti da altri e posti in rete. In queste ipotesi occorrerà riferirsi alla disciplina del diritto d'autore, regolato dalla legge 633/1941, così come modificata dalla legge 248/00. Il reato contempla anche gli illeciti dovuti alla duplicazione, o distribuzione, di programmi utilizzabili con un elaboratore.

Infine, rientrano nella casistica dei reati collegati alla 'rete', quelli connessi alla pedopornografia, introdotti dalla legge n. 269 del 1998, che punisce chi, per via telematica, distribuisce e divulga materiale che ritrae minori in atteggiamenti sessuali, ovvero distribuisce, o divulga, notizie o informazioni con il fine dell'adescamento o dello sfruttamento di minori e chi cede, anche a titolo gratuito, tale materiale e addirittura chi ne disponga.

Per quanto riguarda le 'norme speciali' sono previste disposizioni che tutelano l'integrità dei sistemi informatici e telematici dal danneggiamento (art. 635-bis c.p.) o dalla diffusione di programmi diretti a danneggiarli, o interromperli (art. 615-quinques c.p.). Il legislatore ha altresì introdotto nuove ipotesi di reati quali quelli a tutela del "domicilio informatico" come l'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) e la detenzione, e diffusione, in modalità abusiva, di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.).

[93] Già art. 35 legge 675/1996.

Con l'avvento di internet è stata inoltre introdotta la norma che regola la "frode informatica" (art. 640-ter c.p.) che punisce chi altera un sistema informatico o interviene su dati, informazioni o programmi contenuti in esso per procurare a sé o ad altri un ingiusto profitto.

Il D.lgs n.231/2001, ha introdotto la (cd. responsabilità amministrativa da reato)[94] che inerisce alla responsabilità per gli illeciti amministrativi. Il decreto prevede un elenco di reati che, se commessi contro lo Stato, o altro ente pubblico, dalle persone indicate all'art. 5, (appartenenti a "enti forniti di personalità giuridica", "società" e "associazioni anche prive di personalità giuridica") rispondono gli stessi enti in termini di sanzioni.

La frode informatica in danno dello Stato o di altro ente pubblico è uno dei reati introdotti dal decreto. Solo se sono state adottate procedure di vigilanza e controllo, indirizzate a prevenire il reato, è previsto l'esonero della responsabilità dell'azienda, pertanto, anche in questo caso, come nel caso precedente, inerente generici reati informatici, il controllo non è obbligatorio, ma lo diviene se si vuole beneficiare dell'esonero.

In merito alle misure di sicurezza imposte dal Testo Unico sulla Privacy[95] come si vedrà in seguito, esse riguardano il trattamento di dati personali, con specifiche disposizioni che riguardano i casi che prevedono l'uso di strumenti elettronici.

L'art.34 del T.U. consente all'azienda il trattamento di dati solo se vengono adottate alcune precauzioni, inserite nel "disciplinare tecnico" allegato, tra cui l'utilizzazione di un sistema di autorizzazione e

[94] G. SCIUMBATA, *I reati societari*, Giuffrè, 2002, p.45.

[95] Introdotto con il d.lgs. n.196/03, il Testo Unico è entrato in vigore dal 01.01.2004, ma, come anticipato, con il D.Lgs. n.101 del 2018 è stato integrato.

protezione degli strumenti elettronici e dei dati. Il titolare dell'azienda deve altresì adottare misure di sicurezza "idonee e preventive", tese ad evitare responsabilità sul piano civilistico del risarcimento del danno.

Ciò è previsto nella previsione dell'art.13 del T.U., che rimanda all'art. 2050 c.c. per cui: "*Chiunque cagiona ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee a evitare il danno*"[96].

Poiché lo scambio di e-mail inviate dai dipendenti pone a rischio la *privacy* sia aziendale che soggettiva, occorre predisporre un meccanismo che consenta la conservazione di tali dati. Un'eventuale controllo delle mail può essere giustificato, dunque, dalla necessità di assicurare il rispetto della privacy.

Relativamente ai reati commessi 'su Internet', la Legge n. 547/1993 ha inserito due nuove fattispecie di reato prevedendo che: «*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*

---

[96] *Il legislatore ha preso evidentemente in considerazione il fenomeno di quelle attività le quali sono, per la loro intrinseca pericolosità, in grado di generare con larga probabilità dei danni e nello stesso tempo tuttavia sono ritenute lecite per la loro rilevante utilità sociale. Ovviamente sussiste la necessità, data la effettiva pericolosità di alcune attività, che l'esercente adotti tutte. quelle che sono reputate le misure idonee ad evitare gli eventi dannosi. A seguito dell'emanazione di detta norma contenuta nell'art. 2050 c.c. del codice civile del '42, sia la dottrina che la giurisprudenza dell'epoca, avevano ritenuto che si fosse potuto trattare di una responsabilità soggettiva e cioè ancorata alla colpa o al dolo dell'agente. Si indagava ancora, infatti, sul comportamento del soggetto esercente l'attività pericolosa. Su queste basi i primi esiti giurisprudenziali erano stati improntati dunque verso una responsabilità di tipo soggettivo (….)Tuttavia, come fa notare certa autorevole dottrina in merito, si è ormai pervenuti ad un concetto o unitario di colpa per il quale si tiene conto dell'uomo di media e normale diligenza – bonus pater familias -. Si dice cioè che l'uomo accorto e prudente e cioè il cd. buon padre di famiglia, quando esercita attività pericolose, di sicuro pone in atto tutte quelle misure che sono possibili affinché possano essere evitati eventuali eventi dannosi.* G. GENTILINI, *Cenni sulla responsabilità derivante dall'esercizio di attività pericolose con specifico riguardo alle fonti di elettromagnetismo*., Dicembre 2001, in:*www.diritto.it.*

chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni»; «*Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni*»[97].

In una sentenza emessa dal Tribunale di Roma nel 2002[98]è stato dichiarato il non luogo a procedere nei confronti di un utente che si era introdotto via Internet '*nel sito telematico del GR1, rinominandolo con lo stesso nome di quello autentico*'. In tale occasione, il Giudice ha ritenuto che il legislatore, con l'art. 615-ter, ha inteso tutelare non la *privacy* di qualsiasi "domicilio informatico", ma quella di sistemi "protetti" contro il pericolo di accessi da parte di persone non autorizzate.

Quanto descritto evidenzia che gli strumenti informatici potrebbero permettere controlli talmente invasivi da compromettere la dignità e la riservatezza dell'azienda e del dipendente ma, al contempo, che il traffico telematico espone alla commissione di reati che le aziende sono tenute ad impedire. Nel prosieguo verranno analizzati i dispositivi sul tema assumendo, fin d'ora, che essi mirano a salvaguardare e a contemperare gli interessi vicendevolmente coinvolti: quelli dell'azienda tenuta ai controlli e quelli dei lavoratori.

[97] Articoli 615-ter e 615-quater.

[98] Ufficio del Giudice per le indagini preliminari, sez. 8° , n. 12005/98 R.G., notizie di reato n. 6677/99 R.G.G.I.P.

2.2 I limiti al controllo del traffico telematico nella Convenzione Europea per la salvaguardia dei Diritti dell'Uomo

Presupposti per stabilire i principi su cui basare il controllo delle modalità d'impiego degli strumenti telematici in azienda da parte dei lavoratori, sono rinvenibili anche negli articoli della CEDU (Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo) e delle libertà fondamentali, in particolare gli articoli 8 e 10.[99]

L'art. 8 CEDU stabilisce quanto segue:

1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.

2. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non laddove tale ingerenza sia contemplata dalla legge in quanto provvedimento che, in una società democratica, risulti necessario per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui.

L'uso delle mail private in ambito lavorativo trova una disciplina nell'art.8 che contiene un presupposto applicativo, visto che dall'accezione alla protezione della "vita privata" sancita dall'articolo non esulano gli ambiti professionali, né la vita al di fuori delle mura domestiche. Ne è una conferma il caso 'Niemitz contro Germania',

[99] Rientrano nei diritti assoggettabili a limitazioni non espressamente indicate e quindi lasciate alla discrezionalità delle autorità statali, ma sindacabili dalla Corte europea sotto il profilo della proporzionalità, legalità, conformità e necessarietà rispetto al conseguimento di uno scopo preciso (art. 8 diritto al rispetto della vita privata e familiare; art. 9 libertà di pensiero, di coscienza e di religione; art. 10 libertà di espressione; art. 11 libertà di riunione e di associazione.

sottoposto alla Corte EDU **che** riguardava la perquisizione dell'ufficio del ricorrente effettuata dall'autorità governativa.

Nel caso in discussione, la Corte ha ritenuto che: *"Del rispetto della vita privata deve parimenti far parte in certa misura il diritto di stabilire e sviluppare relazioni con altri esseri umani. Non sembra inoltre esservi alcuna ragione di principio per la quale si debba considerare tale interpretazione della nozione "vita privata" tale da escludere attività di natura professionale o commerciale, giacché dopo tutto è nel corso della propria vita lavorativa che la maggior parte delle persone ha una possibilità significativa, se non la più significativa, di sviluppare relazioni con il mondo esterno. Questa tesi è confortata dal fatto che, come la Commissione ha correttamente fatto rilevare, non è sempre possibile distinguere chiaramente quali tra le attività svolte da un individuo rientrino nell'ambito della sua vita professionale o commerciale e quali no*[100]*"*

In un altro caso, 'Halford contro Regno Unito', la Corte EDU ha chiarito che l'intercettazione delle telefonate dei dipendenti sul posto di lavoro, risultando simili alla violazione della corrispondenza, costituisce una violazione dell'articolo 8 della Convenzione.

Il governo britannico proponeva la tesi che riteneva che, per le chiamate telefoniche effettuate dal lavoratore dal suo posto di lavoro non valesse la protezione accordata dall'articolo 8 poiché nell'effettuarla non si poteva pretendere alcuna riservatezza. A parere della Corte, invece, *"risulta chiaro dalla giurisprudenza che le chiamate telefoniche effettuate da sedi commerciali possano, alla pari di quelle effettuate da casa, rientrare nell'ambito*

[100] Corte EDU, 23 novembre 1992, serie A n. 251/B, paragrafo 29, in: www.garanteprivacy.it

delle nozioni di "vita privata" e "corrispondenza" a termini dell'articolo 8, paragrafo 1 (omissis).

In merito al primo comma dell'art.8 occorre concludere che, nella nozione di "corrispondenza", rientrano non soltanto lettere scritte su carta, ma anche, altre forme di comunicazione quali chiamate telefoniche ovvero *e-mails* ricevuti od inviati per mezzo dei *computers* .

Alcuni interpreti ritengono che, se un dipendente viene avvisato in anticipo dal datore, circa la possibilità di essere intercettato, egli possa accettare di perdere le aspettative di riservatezza (e in tal caso le intercettazioni non costituirebbero una violazione dell'articolo 8 della CEDU).[101]

Inoltre, la tutela della vita privata comprende anche il diritto a stabilire, e sviluppare, relazioni con altri esseri umani e ciò pone alcuni limiti alle legittime esigenze del datore di lavoro in fatto di provvedimenti di vigilanza. Anche l'art. 10, come anticipato, ha rilevanza sul tema, stabilendo che:

1. Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni od idee senza ingerenza alcuna da parte delle autorità pubbliche ed indipendentemente dalle frontiere. Il presente articolo non impedisce che gli Stati sottopongano ad un regime di autorizzazione le imprese di radiodiffusione, di cinema o di televisione.

2. L'esercizio di queste libertà, comportando doveri e responsabilità, può essere sottoposto a determinate formalità, condizioni, restrizioni o sanzioni disposte dalla legge e necessarie in una società democratica per la sicurezza nazionale,

[101] S. BARTOLE , P. DE SENA , V. ZAGREBELSKY, *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, CEDAM, 2012, pp.. 38 –40.

l'integrità territoriale o l'ordine pubblico, la prevenzione di disordini e reati, la protezione della salute o della morale, la protezione della reputazione o dei diritti altrui, oppure per impedire la divulgazione d'informazioni confidenziali oppure ancora per garantire l'autorità e l'imparzialità del potere giudiziario.

L'articolo 10 CEDU prevede,dunque, il diritto a ricevere e a fornire informazioni ed idee senza interferenze da parte delle autorità pubbliche. Il 'caso Niemitz contro Germania' conferma tale aspetto, prevedendo che sul posto di lavoro le persone sviluppano una parte significativa delle loro relazioni ed è quindi indubbio che esse vadano tutelate anche in tale ambito.

2.3 La Direttiva 46/95 CE e l'art. 29 WP

La Direttiva 46 del 1995 (che il Regolamento UE 2016/679 ha sostituito, integrandone i contenuti principali) si pone il fine di regolare il trattamento dei dati personali e la loro diffusione[102]. Tra i vari principi introdotti rileva quello della 'finalità', che prevede che i dati personali vadano raccolti per uno scopo determinato che, oltre a dover essere legittimo, deve essere reso esplicito. Inoltre, tali dati non possono essere trattati conservati per essere trattati in un secondo momento in modo incompatibile con le finalità precedentemente indicate. Il principio della 'trasparenza', invece,esclude qualsiasi controllo occulto della posta elettronica da parte del datore, fatti salvi i casi in cui una legge dello Stato

[102] Sulla storia dello sviluppo del diritto alla privacy: F. PIZZETTI , *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016.

membro lo consenta[103]. Ciò ha maggiore probabilità di verificarsi nei casi in cui si è individuata una specifica attività in cui tale controllo si rende necessario, ovvero in cui le disposizioni nazionali, che stabiliscono le necessarie salvaguardie autorizzino il datore ad agire per rilevare eventuali infrazioni alla legge sul posto di lavoro.

Per quanto attiene alla 'trasparenza' è necessario garantirla fornendo informazioni al titolare dei dati circa la politica aziendale relativa al controllo della posta elettronica e di internet. Ai lavoratori è necessario fornire informazioni complete circa le circostanze che giustificano tale provvedimento eccezionale, chiarendo l'ampiezza di tali controlli. Le informazioni da rendere dovrebbero essere relative ad alcuni aspetti specifici, quali:

1. la politica aziendale perseguita in tema di *e-mail* ed Internet, allegando la descrizione della misura in cui le infrastrutture telematiche possono venire utilizzate dai lavoratori per comunicazioni personali o private (ad esempio limiti di durata dell'impiego);

2. motivi e finalità di una vigilanza eventuale; in tal senso, laddove il datore abbia consentito espressamente l'impiego delle infrastrutture di comunicazione per finalità private, le comunicazioni di natura personale possono essere ridotte, ad esempio, per garantire la sicurezza del sistema d'informazione;

---

[103] L'articolo 13 della direttiva consente ai Paesi membri di prendere provvedimenti per ridurre l'ambito applicativo degli obblighi e dei diritti stabiliti da alcuni articoli, se tale misura è necessaria a salvaguardare interessi pubblici, oppure di prevenire, indagare perseguire possibili reati.

4. le procedure volte a garantire il rispetto delle regole, e delle possibilità offerte ai dipendenti per rispondere alle accuse eventualmente mosse contro di loro.

L'art.29 della Direttiva prevede l'istituzione di un gruppo di lavoro di natura consultiva sul tema del trattamento dei dati.

Il Gruppo di lavoro art.29 (WP art.29) è' un organismo consultivo indipendente, composto da un rappresentante della varie autorità nazionali, dal Garante europeo della protezione dei dati, e da un rappresentante della Commissione. Il presidente è deciso al suo interno ed ha un mandato di due anni, rinnovabile una sola volta.

Il Gruppo adotta le sue decisioni a maggioranza semplice ed è stato successivamente, sostituito, nelle sue funzioni, dal Comitato europeo per la protezione dei dati, *European data Protection Board*[104].

Tra le varie interpretazioni, il Gruppo di lavoro ha ritenuto che, sotto il profilo pratico, è sempre consigliabile informare il dipendente di qualsiasi uso improprio delle comunicazioni elettroniche rilevato in azienda. Tali informazioni potrebbero essere rese, secondo il Gruppo di lavoro, con dispositivi *software* (quali finestre contenenti avvertimenti, da fare apparire sullo schermo in cui si avvisa il lavoratore che il sistema ha

[104] Le funzioni dell'ente sono di fornire indicazioni generali (comprese linee guida, raccomandazioni e migliori prassi) per chiarire la legge sulla privacy; consigliare la Commissione europea su qualsiasi questione relativa alla protezione dei dati personali e alla nuova legislazione proposta nell'Unione europea; controllare la coerenza nei casi di protezione dei dati transfrontalieri; e promuovere la cooperazione e l'effettivo scambio di informazioni e best practices tra le autorità di vigilanza nazionali. L'ente pubblica una relazione annuale sulle attività, che è resa pubblica e inviata al Parlamento europeo, al Consiglio e alla Commissione. I principi guida dell'ente sono: Indipendenza e imparzialità Buon governo, Integrità e buon comportamento amministrativo, Collegialità, Cooperazione Trasparenza, Efficienza e modernizzazione e Proattività.

segnalato un uso non autorizzato della rete).Tali comunicazioni potrebbero coinvolgere anche i rappresentanti dei lavoratori[105].

Gli accordi collettivi aziendali possono, inoltre, arrivare a stabilire il campo d'applicazione e la portata dell'impiego di Internet e della posta elettronica consentito ai dipendenti, nonché i gli aspetti pratici relativi al controllo di tale impiego. La direttiva 46/95 ha altresì introdotto l'obbligo d'informare le autorità di vigilanza, prima di procedere a qualsiasi operazione di trattamento dei dati in modalità (parzialmente od integralmente) automatica. Inoltre, in forza della direttiva 95/46/CE un lavoratore dipendente ha il diritto di accedere ai dati personali trattati dal suo datore e richiederne la rettifica, oppure la cancellazione o il congelamento, laddove le informazioni rese dovessero rilevarsi incompleti o inesatte[106].

---

[105] Le decisioni in tema di controlli, inclusa la sorveglianza delle comunicazioni elettroniche effettuate o ricevute, rientrano nel campo d'applicazione della direttiva 2002/14/CE che stabilisce la necessità d'informare e consultare i lavoratori in merito alle decisioni atte a determinare cambiamenti sostanziali nell'organizzazione del lavoro o nelle relazioni contrattuali.

[106] Articolo 12: gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento:

a) liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi:

- la conferma dell'esistenza o meno di trattamenti di dati che la riguardano, e l'informazione almeno sulle finalità dei trattamenti, sulle categorie di dati trattati, sui destinatari o sulle categorie di destinatari cui sono comunicati i dati;

- la comunicazione in forma intelligibile dei dati che sono oggetto dei trattamenti, nonché di tutte le informazioni disponibili sull'origine dei dati;

- la conoscenza della logica applicata nei trattamenti automatizzati dei dati che la interessano, perlomeno nel caso delle decisioni automatizzate di cui all'articolo 15, paragrafo 1;

b) a seconda dei casi, la rettifica, la cancellazione od il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto od inesatto dei dati;

c) la notificazione ai terzi ai quali sono stati comunicati i dati di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera b), se non si dimostra che è impossibile o implica uno sforzo sproporzionato.

Un ulteriore principio introdotto dalla Direttiva è quello della 'legittimità', che subordina la possibilità di svolgere qualsiasi operazione di trattamento dati alla condizione che essa persegua fini legittimi, ome sancito dall' articolo 7 della direttiva 95/46/CE[107].

L'articolo 7, alla lettera f) della direttiva dispone, infatti, che il trattamento dei dati riguardanti un lavoratore dipendente può essere consentito solo se viene finalizzato al perseguimento di interessi legittimi e quando non infrange i suoi diritti fondamentali.

Il trattamento di 'dati delicati' connessi ad attività di vigilanza e controllo viene considerata un'eccezione, in quanto generalmente inaccettabile, a meno che tale pratica non dovesse essere specificamente autorizzata da disposizioni nazionali di legge tali da offrire adeguate garanzie.

In merito al principio di 'proporzionalità' stabilito dalla direttiva, si esclude la possibilità di effettuare un controllo fitto circa l'impiego della posta elettronica e di Internet da parte del personale. Il principio, dunque, postula che tali controlli avvengano solo se necessari.

Pertanto il controllo deve essere realizzato in modo poco intrusivo ed evitando di ricorrere a sistemi che effettuino controlli automatici e persistenti.

Inoltre, ad avviso del Gruppo di lavoro art.29, il controllo della posta elettronica privata dovrebbe limitarsi ai dati riguardanti l'entità dello scambio di corrispondenza e la durata delle comunicazioni, piuttosto che al contenuto di queste ultime. Nell'accedere alla posta elettronica si dovrà, inoltre, tener conto della sfera privata non solo degli appartenenti

[107] E delle disposizioni con le quali essa è stata recepita nelle legislazioni nazionali.

all'organizzazione, ma anche delle persone che ricevono i messaggi in questione. Il datore di lavoro, in questi casi, dovrà fare quanto in suo potere per informare i corrispondenti esterni all'organizzazione dell'esistenza di attività di controllo.

Un esempio pratico, suggerito dal Gruppo di lavoro art.29, potrebbe essere l'inserimento di avvertenze riguardanti l'esistenza del sistema di controllo in tutti i messaggi indirizzati a destinatari esterni all'organizzazione. Un messaggio dedicato non sembra idoneo allo scopo, risultando una misura non commisurata agli obiettivi perseguiti, per cui i dispositivi di blocco del contenuto, in presenza di tali avvisi devono ritenersi preferibili a quelli di controllo[108].

In base al principio di proporzionalità i sistemi per il trattamento delle comunicazioni elettroniche andrebbero progettati in modo tale da limitare al minimo necessario la quantità di dati personali trattata. Alcune imprese si avvalgono di un sistema automatico di rinvio ad un *server* isolato per tutti i messaggi di posta elettronica che superino una determinata lunghezza. In questo caso, il destinatario viene automaticamente informato che un messaggio sospetto è stato reindirizzato a tale *server* e può esservi consultato. Per quanto attiene all'uso di internet per scopi di navigazione personale, si raccomanda di usare strumenti *software* utili per bloccare qualsiasi collegamento a categorie predeterminate di siti Web.

La direttiva 95/46 prevede che i dati raccolti dalle imprese vengano conservati con accuratezza. In ossequio a questo principio qualsiasi dato

[108] Laddove tali soluzioni dovessero essere introdotte è necessario informare i lavoratori.

legittimamente archiviato da un datore riguardanti l'indirizzo elettronico dei dipendenti, nonché l'impiego di Internet, devono risultare aggiornati nonché accurati e non possono essere conservati per un periodo superiore al necessario. In tal senso, il datore, nel rendere le informazioni riguardanti le proprie policy di vigilanza, dovrà chiarire quale sia il periodo di conservazione dei messaggi di posta elettronica sul proprio *server* in funzione delle esigenze dell'impresa[109].

Infine, la direttiva ha introdotto il principio della 'sicurezza' che obbliga il datore a prendere i provvedimenti tecnici ed organizzativi del caso per garantire che qualsiasi informazione personale detenuta risulti protetta[110].

Sul tema, il Gruppo di lavoro art. 29 ha ritenuto che, pur considerando l'importanza della sicurezza, l'apertura automatizzata dei messaggi di posta elettronica non debba considerarsi tale da violare il diritto dei lavoratori dipendenti alla *privacy*.

Il Gruppo sollecita la creazione in azienda del ruolo di amministratore del sistema, da affidarsi ad un dipendente con considerevoli responsabilità sotto il profilo della protezione dei dati.

Nelle ipotesi in cui intenda avvalersi di una procedura *Data Loss Prevention*, finalizzato al recupero dei dati per non perderli, il datore deve prima informare tutti i lavoratori dell'impresa.

Inoltre, in tal caso, occorre determinare, adottando regole di chiarezza, le modalità rispetto alle quali il sistema informatico classifica una e-mail in uscita in grado di violare la riservatezza aziendale e, nell'eventualità in

[109] Di norma risulterà difficile giustificare un periodo di conservazione superiore ai tre mesi.

[110] Ciò può anche comportare una scansione automatizzata dei dati relativi ai messaggi di posta elettronica ed al traffico Internet.

cui si dovesse determinare un caso di violazione, si suggerisce di informarne l'interessato[111].

L'utilizzo della strumentazione informatica da remoto che espone al rischio di accessi ai dati personali da parte di terzi non autorizzati, il datore non può adottare misure di sicurezza quali webcam o tecnologie di "screen capture" o , addirittura, sistemi che rilevino i movimenti del mouse, poiché ritenuti non proporzionati.

È, invece, possibile porre in essere misure di sicurezza che rispettino la riservatezza degli interessati[112].

2.4 Il controllo telematico dei lavoratori nell'art. 4 dello Statuto dei lavoratori. Le novità apportate con il Jobs Act

Nel capitolo precedente è stato ampiamente illustrato il contenuto dell'art. 4 dello Statuto dei lavoratori. In questa fase del l'elaborato che sviluppa le fonti da cui è possibile trarre la disciplina relativa all'uso di internet da parte dei dipendenti, risulta utile focalizzare

[111] Ciò al fine di consentire a quest'ultimo di cancellare, e non inviare ,tale comunicazione.

[112] Ad esempio, se si intende accedere agli *smartphone* dei dipendenti, a causa ad esempio perdita di dati personali, il datore di lavoro non può accedere ad aree ritenute "private", come, ad esempio, l'archivio fotografico. Tramite le tecnologie di Mobile Device Management è possibile al datore di lavoro la gestione da remoto di dispositivi mobili dei lavoratori. Al fine di verificare la necessità del trattamento rispetto alle finalità perseguite sarebbe opportuno una DPIA prima dell'avvio del trattamento, in modo da garantire il rispetto dei principi di proporzionalità e sussidiarietà. In questo caso si dovrebbe dimostrare in primis che il ricorso a tali tecnologie informatiche non rientra in un programma più ampio volto al controllo dei lavoratori. Inoltre, il controllo dei dispositivi mobili dovrà ritenersi un'ultima istanza cui far fronte solo in casi eccezionali come nel caso di smarrimento.

le integrazioni apportate dal legislatore, intervenuto nel 2015 a per ridisegnare i rapporti tra datori e lavoratori. In particolare, l'art.23 del D. Lgs 151 del 2015 ha introdotto alcune novità nel dispositivo dell'articolo, tanto che ora risulta così formulato:

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 2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze 3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.

L'analisi delle integrazioni (indicate con sottolineatura) evidenzia un maggior potere assegnato al datore di lavoro e, al contempo, riconosce un nuovo ruolo al *Garante della Privacy*. Infine, il lavoratore ha ricevuto una maggior tutela visto che, oggi la norma prescrive che le condizioni per l'uso delle "informazioni raccolte" ai sensi dei commi 1 e 2 sono: *a)* l'aver fornito adeguata informazione delle modalità d'uso degli strumenti stessi e di effettuazione dei controlli e *b)* che venga rispettato tutto l'apparato di regole procedurali e tutele dettate dal *Codice privacy*[113]. La Circolare n.20 del 2015 emessa dalla Fondazione Studi dei Consulenti del lavoro ha chiarito che gli strumenti che "servono al lavoratore" per rendere la prestazione lavorativa sono quelli necessari e serventi a tale scopo e non quelli che servono per realizzare funzioni differenti. Permane un esplicito divieto di utilizzo di apparecchiature o strumenti con finalità esclusiva di controllo a distanza[114].

Per quanto riguarda l'art.4 dello Statuto, la scomparsa dell'esplicitazione del divieto di compiere controlli sull'attività dei lavoratori mostra un cambio di prospettiva nell'approccio sistematico alla materia. Considerando gli impianti audiovisivi e gli strumenti di cui il datore di lavoro ritenga di doversi dotare per esigenze diverse rispetto all'esecuzione della prestazione lavorativa, il legislatore ha confermato, nel 2015, la non tolleranza del loro uso per controllare l'attività lavorativa. Rispetto agli strumenti di lavoro, invece, oggi il legislatore ha la possibilità di operare qualsiasi tipo di controllo, fermi i limiti della rilevanza

[113] A. SITZIA, *Il controllo (del datore di lavoro) sull'attività dei lavoratori,* LLI, Vol. 2, No. 1, 2016, ISSN: 2421-2695, 86.

[114] Che appare rinforzata dall'impossibilità di eludere qualsiasi *privacy* anche di non stretta derivazione lavorativa.

ai fini della valutazione dell'attitudine professionale (art. 8 St. lav.), del rispetto della dignità del lavoratore, della riservatezza sua e dei terzi coinvolti, e della tutela generale civilistica in materia di *privacy*. Nel 2015 il legislatore ha inteso considerare 'ormai consolidato sviluppo e diffusione delle tecnologie nella vita quotidiana e lavorativa ammettendo che gli strumenti di lavoro non producano più un'invasione molesta e intollerabile nella propria sfera personale, essendone divenuti, spesso, delle mere strumentazioni.

Il Jobs Act ha stabilito che ciascuna azienda sia tenuta a redigere un documento che illustri la *'Policy sulla sicurezza informatica'* in cui si delineano i comportamenti richiesti ai dipendenti per contrastare i rischi informatici, quali l'esternazione di segreti. In mancanza di tale documento, il datore si sottopone all'obbligo di fornire prova che l'attività lesiva sia stata posta in essere dal lavoratore dipendente in pendenza dell'orario di lavoro, nonostante precedenti richiami e abbia comportato un danno all'azienda di entità rilevante[115].

Il combinato disposto dei primi due commi dell'art. 4 lascia, dunque, un ampio margine per l'esplicarsi del potere di controllo tecnologico sugli strumenti di lavoro, non essendo più nemmeno necessaria l'installazione di programmi di controllo *specifici* per rendere possibile monitoraggio dell'attività dei lavoratori.

Gli strumenti di lavoro informatico/tecnologici, infatti, sono naturalmente dotati di una i capacità di immagazzinare,

[115] Le sentenze emesse dalla Corte di Cassazione (che verranno illustrate nel prossimo capitolo) evidenziano che solo la reiterata condotta, con portata lesiva grave, è idonea a giustificare la massima sanzione disciplinare del licenziamento.

attraverso i c.d."*file log*", la sequenza nonché la cronologica delle operazioni effettuate[116].

Gli stessi lavoratori non percepiscono più la nuova realtà tecnologica come causa di possibili attentati alla propria sfera personale. È legittimo affermare che vi sia, oggi, una sovrapposizione tra "strumento di lavoro" e "strumento di controllo", che fa sì che il controllo sugli strumenti utilizzati non siano più soggetti ad alcun limite. Resta fermo che il trattamento dei dati raccolti attraverso l'esercizio del controllo permane assoggettato ai principi di finalità[117], liceità, legittimità e non eccedenza, stabiliti dal *Codice privacy*.

2.5 L'uso di internet da parte del lavoratore nella disciplina del codice civile

I controlli aziendali mirati devono tendere a verificare l'adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.)

L' art. 2086 disciplina la 'Direzione e gerarchia nell'impresa' e stabilisce che '*L'imprenditore è il capo dell'impresa e da lui dipendono gerarchicamente i suoi collaboratori'* attribuendogli, così, un potere sui lavoratori che gli

[116] A. TROJSI, *Il comma 7, lettera f) della legge delega n. 183/2014. Tra costruzione del Diritto del lavoro dell'era tecnologica e liberalizzazione dei controlli a distanza sui lavoratori*, in M. Rusciano et al., *Jobs Act e contratti di lavoro dopo la legge delega 10 dicembre 2014*, n. 183, W.P. CSDL "Massimo D'Antona", http://csdle.lex.unict.it/, collective.

[117] Specificato dall'art. 4 medesimo nel senso che le finalità ammesse sono quelle connesse al rapporto di lavoro.

dipendono[118]. Il potere del datore di organizzare i lavoratori concorre con quello di auto organizzarsi consentendogli di stabilire le modalità con cui gestire le attività d'impresa.

In tale ottica, il datore ha il potere di emanare il regolamento aziendale in cui inserire le regole cui sottostare che, comunque, non possono essere contrarie alle disposizioni di legge. Inoltre, il regolamento non può configgere con il dispositivo dell'art. 2087 c.c. che disciplina la 'Tutela delle condizioni di lavoro'.

Tale articolo stabilisce che '*L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro'*. Ciò implica che nessuna misura di natura direttiva o relativa al monitoraggio delle attività, possa minare alla dignità ed alla integrità fisica dei dipendenti, ciò anche se tali misure implichino il coinvolgimento della strumentazione informatica. L'azienda che osserva la '*policy* sulla sicurezza informatica', facendo effettuare l'analisi dei rischi lavorativi, e di quelli informatici, opera in accordo con l'articolo 2087 c.c. che regola l'adempimento degli obblighi in materia di sicurezza sul lavoro.

Le attività di controllo informatico del datore sono rafforzate, d'altro canto, dal dispositivo dell'art 2104 c.c. che regola la 'Diligenza del prestatore di lavoro' stabilendo che '*Il prestatore di lavoro deve usare la diligenza richiesta dalla natura della prestazione dovuta, dall'interesse*

[118] In tal senso rileva la sent. Cassazione Civile, sez. lavoro, 10 luglio 2009, n. 16196, secondo cui. '*E' lecito pedinare il dipendente per controllare la prestazione, ma la prova del grave inadempimento è, in ogni caso, a carico del datore di lavoro*'.

dell'impresa e da quello superiore della produzione nazionale. Deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende'.

L'art. 2104 c.c. va interpretato anche considerando quanto stabilito dall'art.. 2105 c.c. che impone al lavoratore l'obbligo di fedeltà che può desumersi anche dalle modalità di impiego degli strumenti informatici, nonché dal loro contenuto. I danni derivanti dall'eventuale mancata osservanza di quanto disposto dai due articoli comporta un 'danno patrimoniale' per il datore.

Il datore ha, altresì, il diritto di pretendere la diligenza del lavoratore, ai sensi dell'art.1176 c..c..Quest'ultima individua le modalità dell'esecuzione della prestazione ma anche la responsabilità. In definitiva, tutti gli articoli citati possono essere considerati una guida per la definizione della giusta condotta aziendale in costanza di controlli sull'uso di internet in azienda. Si tratta, infatti, di principi che sottopongono il datore ad obblighi precisi, contemperandoli agli interessi aziendali citati.

2.6 Il Testo Unico sulla Privacy ed il controllo dell'uso di internet in azienda

Sotto il profilo del rapporto di lavoro, la disciplina della *privacy* è ritenuta generale, rispetto quella speciale statutaria[119]; per cui il datore, una volta acquisiti i dati personali del lavoratore nel rispetto delle disposizioni,

[119] P. LAMBERTUCCI, *Svolgimento del rapporto di lavoro e tutela dei dati personali*, in AA.VV. *La tutela della privacy del lavoratore*, UTET, 2001, p.97.

dovrà confrontarsi con le prescrizioni generali poste a tutela della sfera della riservatezza del dipendente[120].

Come è stato ampiamente illustrato il monitoraggio degli accessi internet dei lavoratori implica la conoscenza di un'innumerevole quantità di dati personali per cui è necessario risalire alla normativa posta nell'ambito della legislazione sulla protezione dei dati[121].

Al pari della legge 675 del 1996, anche il Testo Unico sulla *Privacy* impone il rispetto di determinati criteri guida per procedere ad ogni trattamento dei dati personali. Il Regolamento europeo GDPR (General Data Protection Regulation) 2016/679, approvato a settembre 2018, nel sostituire il Codice della *privacy*, ha integrato il TU, preservandone i principi generali che verranno di seguito illustrati. I criteri in oggetto, sono evidenti nell'art. 11 del Testo Unico,e mirano a garantire il rispetto del diritto alla dignità personale, alla riservatezza e, in genere, alle libertà fondamentali dell'individuo.

I dati personali, devono essere raccolti e registrati per scopi determinati, espliciti e legittimi e solo dopo è possibile impiegarli sempre in termini compatibili con tali scopi. I dati oggetto di trattamento devono essere esatti e, se necessario, aggiornati,inoltre devono essere completi e non eccedenti rispetto alle finalità per cui sono stati raccolti.

Una volta raccolti, i dati personali devono essere conservati in una forma che consenta che l'interessato possa visionarli. Inoltre la loro

---

[120] Nel Documento di lavoro del gruppo di lavoro ex art. 29 riguardante la vigilanza ed i controlli sulle comunicazioni elettroniche effettuate dal posto di lavoro, pag. 2; si legge che *il Gruppo – Articolo 29 ha enfaticamente osservato che "quando al mattino si recano a lavorare i lavoratori non abbandonano fuori dell'ufficio o della fabbrica i loro diritti alla riservatezza ed alla protezione dei dati*".

[121] Newsletter 17.09.01 Garante Privacy, in *www.garanteprivacy.it.*

conservazione deve avvenire per un periodo di tempo non superiore a quello necessario per gli scopi per cui sono stati assunti.

Le precauzioni imposte dal Testo Unico sulla *privacy* dovranno essere predisposte in maniera da fungere da garanzia preventiva.

Ai sensi dell'art. 13 del Testo Unico[122] è necessario predisporre un' informativa sul trattamento, nonché la finalità e la modalità con cui realizzarlo.

Il TU considera necessario informare e ricevere l'autorizzazione al trattamento dei dati che, tra l'altro, potrebbero essere attinti da connessioni a siti a sfondo religioso, politico o pornografico.

Tali dati possono essere trattati "*solo con il consenso dell'interessato e previa autorizzazione del Garante*", secondo le modalità ed limiti stabiliti dal Testo Unico, nonché dalla legge e dai regolamenti.

Nel tenore del Testo Unico, segnatamente agli artt. 24 e 26, si riscontrano due casi di esclusione alla regola del consenso, rispettivamente in relazione ai dati personali e ai dati sensibili. L'art. 24 del T.U. stabilisce

[122] Art.13 T.U. sulla privacy: "1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7;
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.".

che:"*il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:*

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;…".

Al comma quarto dell'art. 26, invece, si prevede che "*i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante*:…

quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo."

Ai sensi dell'art. 4 del Testo Unico sulla Privacy per "dati sensibili" si intendono "*i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*."

Fermo restando l'onere all'informativa del trattamento è, pertanto, assodato che il consenso del singolo lavoratore al monitoraggio del traffico telematico personale, non sia ammesso. Anche la dottrina giuslavorista è giunta alla stessa conclusione, assumendo che la disparità

di forza contrattuale (che giustifica le norme statutarie di protezione) eliminerebbe ogni rilevanza al consenso individuale[123].

Con le stesse ragioni si può escludere che sussista l'obbligo, di cui all'art. 26, di chiedere individualmente l'autorizzazione del Garante per procedere al trattamento dei dati sensibili.

L'art. 114 del T.U.[124]contiene una clausola di ultravigenza dello Statuto dei lavoratori prevedendo che, laddove il datore di lavoro abbia raccolto dati sensibili del lavoratore con modalità consentite dallo Statuto, non si applica la disposizione che impone l'autorizzazione del Garante[125].

La Notificazione del trattamento, imposto dal Testo Unico solo nei casi in cui essi riguardano "*dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti*".

Considerando la normale presenza in azienda di strumenti informatici, è logico ritenere che, solo in caso di un'implementazione con appositi *software* della funzione base, il datore sarà tenuto ad adempiere alla notificazione a tutti i lavoratori.

---

[123] P. LAMBERTUCCI, *Svolgimento del rapporto di lavoro e tutela dei dati personali*, in: *La tutela della privacy del lavoratore*, AA.VV. , UTET, 2001, p.102.

[124] Già art. 43, comma 2, della Legge 675/96.

[125] J. MONDUCCI, *Controllo del lavoratore e trattamento dei dati personali*, in: *Diritto e Pratica delle Società*, 2, luglio 2001, Il Sole 24 Ore.

2.7 Le linee guida del Garante per la privacy per l'uso da parte del lavoratore di posta elettronica e internet

Nell'esaminare il tema in oggetto non si può assolutamente prescindere dalle "Linee guida" emanate dal Garante per la privacy con la Delibera n. 13 del 1 marzo 2007, relativamente a "posta elettronica e internet".

In base al principio di correttezza l´eventuale trattamento dei dati, secondo il *Garante per la privacy*, deve essere ispirato ad un canone di trasparenza[126]. Il datore di lavoro pertanto ha l´onere di indicare, in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti e se, e con quali modalità, vengono effettuati controlli.

Il monitoraggio dovrebbe anche sottostare alla disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Il Garante ha altresì invitato i datori di lavoro ad informare circa i limiti di utilizzo, per ragioni personali, dei servizi di posta elettronica o di rete. È ammesso che si possa anche indicare la sola postazione di lavoro da cui poter ricevere o inviare posta elettronica, ovvero indicare l´arco temporale di utilizzo[127]; quali informazioni memorizzare temporaneamente[128]e chi (anche all´esterno) vi può accedere legittimamente; se e quali informazioni sono conservate per un periodo più lungo; quali conseguenze, anche di tipo disciplinare, il datore di

[126] *Art. 4, secondo comma, Statuto dei lavoratori;allegato VII, par. 3 D.Lgs. n. 626/1994 e successive integrazioni e modificazioni in materia di "uso di attrezzature munite di videoterminali", il quale esclude la possibilità del controllo informatico "all´insaputa dei lavoratori*.

[127] Ad es., fuori dall´orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro.

[128] Ad es., le componenti di *file* di *log* eventualmente registrati.

lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet vengono utilizzate indebitamente; se, e in quale misura, il datore si riserva di effettuare controlli in conformità alla legge indicando le ragioni specifiche, mai generiche, per cui verrebbero effettuati..

Il Garante invita, inoltre, a stabilire le varie soluzioni volte a garantire la continuità dell´attività lavorativa in caso di assenza del lavoratore stesso, provvedendo all´attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti.

Il Garante invita a specificare tutte e misure adottate in seno a particolari realtà lavorative che necessitano della tutela del segreto professionale. Infine, invita a chiarire e rendere pubbliche le prescrizioni interne sulla sicurezza dei dati e dei sistemi.

Devono essere, tra l´altro, indicate le principali caratteristiche dei trattamenti, nonché il soggetto, o l´unità organizzativa, a cui i lavoratori possono rivolgersi per esercitare i propri diritti.

Il datore di lavoro può riservarsi di controllare (direttamente, o attraverso la propria struttura) l´effettivo adempimento della

prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro. Nell´esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire l´attività di lavoratori.

Secondo il Garante, il datore di lavoro, utilizzando applicazioni informatiche per esigenze produttive o organizzative o, comunque, per

la sicurezza sul lavoro può avvalersi, legittimamente, di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori.

Il trattamento di dati che ne consegue deve, dunque, intendersi lecito[129].

Inoltre, in applicazione del 'principio di necessità' il datore può procedere alla lettura e alla registrazione sistematica dei messaggi di posta elettronica, arrivando fino all'analisi occulta di computer portatili affidati in uso. Il Garante pone si auspica la plausibilità che il datore adotti tutte le misure *tecnologiche* volte a minimizzare l´uso di dati identificativi (c.d. *privacy enhancing technologies–PETs*). Per quanto attiene alla navigazione in internet, il datore per ridurre il rischio di usi impropri della "navigazione"[130] deve adottare opportune misure per prevenire controlli successivi. Il contenuto dei messaggi di posta elettronica è assistito da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nella protezione della dignità umana. Tuttavia, non appare di facile determinazione se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica per uso personale oppure professionale. É quindi particolarmente opportuno che si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l´utilizzo della posta

[129] Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all´introduzione o alla modifica di sistemi automatizzati per la raccolta e l´utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

[130] 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.

elettronica e l´accesso ad Internet determinando l'ubicazione riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.
È inoltre opportuno che si configurino sistemi o filtri che prevengano eventuali operazioni quali l´*upload* o l´accesso a determinati siti e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato).
Il Garante esorta le imprese ad organizzare un trattamento di dati in forma anonima, o tale da precludere l´immediata identificazione di utenti tramite aggregazioni[131].Per quanto riguarda la conservazione dei dati raccolti si raccomanda che essa sia limitata al perseguimento di finalità organizzative, produttive e di sicurezza.
Ogni forma di controllo è lecita solo se sono rispettati i principi di pertinenza e di non eccedenza. Qualora sussista il pericolo di un evento dannoso, o una situazione di pericolo, al datore è, poi, consentito di adottare misure che consentano la verifica di comportamenti anomali.
In questi casi sono da privilegiare, preliminarmente, i controlli su dati aggregati, riferiti all´intera struttura lavorativa, o a sue aree produttive. L'eventuale controllo anonimo può concludersi con un avviso generalizzato riportante l´invito ad attenersi scrupolosamente a compiti assegnati e ad istruzioni impartite. Tale avviso può essere circoscritto a dipendenti dell'area o settore in cui è stata rilevata l´anomalia. Laddove le anomalie dovessero interrompersi l'effettuazione di controlli individuali non è indicata.

[131] Ad es., con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori.

I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente[132] i dati personali relativi agli accessi ad Internet, e al traffico telematico, la cui conservazione non sia necessaria. L'eventuale conservazione temporanea dei dati relativi all´uso degli strumenti elettronici deve essere dovuta (sempre laddove vi siano esigenze specifiche che la giustifichino) ad una finalità specifica.

Pertanto, in linea generale, un prolungamento dei tempi di conservazione va valutato come eccezionale.

Nel rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it,ecc..) il Garante raccomanda di affiancare quelli individuali (ad esempio, m.rossi@ente.it,) da intendersi finalizzati all'uso privato.

Gli indirizzi mail, di uso aziendale, andrebbero interrotti, in caso di assenza del lavoratore.

In caso di eventuali assenze non programmate (ad es. per malattia improvvisa), qualora il lavoratore non possa attivare la procedura descritta, il titolare del trattamento, potrebbe disporre, sempre che sia necessario, e mediante personale appositamente incaricato, l´attivazione di un analogo accorgimento, avvertendo gli interessati[133].

Una volta introdotto il protocollo indicato dal Garante, l'uso privato degli strumenti informatici non conforme alle precisazioni contenute nel disciplinare, da parte dei dipendenti, esonerano l'azienda dall'incorrere

---

[132]Tramite procedure di sovra registrazione come, ad esempio, la cd. rotazione dei *log file* . Il log file registra le attività effettuate e se un file viene fatto ruotare numero volte, allora occorre eliminare il più vecchio file ruotato.

[133] Ad es., l´amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati.

nel reato penale ex art. 616 c.p. (violazione di corrispondenza privata), nel caso specifico *sub specie* di cognizione della posta elettronica indirizzata al dipendente.

Ciò in quanto il reato penale in questione riguarda la cognizione della corrispondenza cd. "chiusa" e non già a quella cd. "aperta", tra cui la Cassazione fa rientrare le comunicazioni via e-mail dei lavoratori dipendenti tramite mail aziendale, in quanto, se anche protetto da password, quest'ultima deve essere comunicata e detenuta in busta chiusa dal Responsabile o preposto del dipendente, legittimato all'utilizzo in casi di emergenza o di assenze prolungate del lavoratore

Nell'eventualità di un'assenza prolungata, in caso di necessità, ovvero nell'esigenza di conoscere il contenuto dei messaggi di posta elettronica, il lavoratore deve delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli rilevanti per consentire il regolare svolgimento dell´attività lavorativa[134].

I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati possono altresì effettuare il trattamento dei dati personali diversi da quelli sensibili.

In particolare, ciò, può avvenire:

a) in caso di valida manifestazione di un libero consenso;

b) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (*art. 24, comma 1, lett. f) del Codice*);

[134] A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile.

c) anche in assenza del consenso, ma per effetto del provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi.

CAPITOLO III

L'UTILIZZO DI INTERNET IN AMBITO AZIENDALE NELLE PRONUNCE GIURISPRUDENZIALI

CAPITOLO III

L'UTILIZZO DI INTERNET IN AMBITO AZIENDALE NELLE PRONUNCE GIURISPRUDENZIALI

3.1 L'uso di internet da parte del lavoratore, evoluzione interpretativa nelle sentenze della Corte di Cassazione

L'accesso da parte del datore di lavoro (o del superiore gerarchico) alla mail aziendale del dipendente può essere necessario per garantire l'adempimento di attività lavorative.

Il tema è giunto più volte dinanzi ai giudici che sono stati chiamati a risolvere questioni in cui i monitoraggi in oggetto hanno portato a soluzioni del rapporto lavorativo ovvero a sanzioni disciplinari.

Il tema dell'accesso alla posta elettronica aziendale è stato oggetto di varie sentenze, non solo della Suprema Corte di Cassazione ma, altresì, dalle corti d'appello. Il Tribunale di Chivasso con sentenza emessa il 15.9.2006[135], stabiliva che: «*Le attrezzature lavorative e, tra queste, quelle informatiche, devono considerarsi direttamente correlate alla funzione del soggetto che rappresenta l'impresa e, solo in via mediata, devono reputarsi assegnate al singolo dipendente, comunque fungibile nel rapporto con lo strumento aziendale. L'indirizzo di posta elettronica aziendale, al di là dell'uso*

[135] Tribunale di Torino, Sezione Distaccata di Chivasso, Sentenza 20 giugno 2006 (dep. 15 settembre 2006), n. 143, in:*www.penale.it*

solo apparentemente personale da parte del dipendente quale principale utilizzatore aziendale, può sempre essere a disposizione di soggetti diversi, appartenenti alla sua stessa impresa. Anche se nell'estensione dell'indirizzo di posta elettronica compare il nome del dipendente che procede all'invio, i messaggi inviati attraverso l'e-mail aziendale rientrano nel normale scambio di corrispondenza che l'impresa intrattiene. Pertanto, in caso di accesso alla casella di posta elettronica aziendale del dipendente da parte dell'impresa, non può ravvisarsi una violazione dell'art. 616 c.p., che contempla il reato di violazione, sottrazione e soppressione di corrispondenza. Non sussiste, infatti, un diritto esclusivo del lavoratore ad accedere in via esclusiva al proprio computer aziendale e ad utilizzare in via esclusiva e riservata la propria casella di posta elettronica aziendale».

Riprendendo la sentenza precedente la Cass. con sentenza n. 47096 emessa il 19 dicembre 2007[136], ha stabilito che: «*Non integra il reato di cui all'art. 616 cod. pen. la condotta del superiore gerarchico che prenda cognizione della posta elettronica contenuta nel computer del dipendente, assente dal lavoro, dopo avere a tal fine utilizzato la password in precedenza comunicatagli in conformità al protocollo aziendale*».

Sempre in ambito di giurisprudenza d'appello, rileva la sentenza emessa dal tribunale di Torino, in cui si stabilisce che: «*Il dipendente che utilizza la casella di posta elettronica aziendale si espone al rischio che anche altri della medesima azienda - unica titolare del predetto indirizzo - possano lecitamente accedere alla casella in suo uso non esclusivo e leggerne i relativi messaggi in entrata e in uscita ivi contenuti, previa acquisizione della relativa password, la*

[136]Cass.Pen., sez. V, sent.19 dicembre 2007, n. 47096, in:www.altalex.it

cui finalità non risulta essere allora quella di proteggere la segretezza dei dati personali custoditi negli strumenti posti a disposizione del singolo lavoratore, bensì solo quella di impedire che ai suddetti strumenti possano accedere anche persone estranee alla società. Ne deriva quindi che, in caso di accesso alla posta elettronica aziendale del dipendente, non sembra dunque potersi ravvisare un elemento essenziale della fattispecie delittuosa di cui all'articolo 616 del Cp rappresentato, sotto il profilo oggettivo, dalla alienità della corrispondenza medesima, apparendo infatti corretto ritenere che i messaggi inviati tramite l'e-mail aziendale del lavoratore rientrino nel normale scambio di corrispondenza che l'impresa intrattiene nello svolgimento della propria attività organizzativa e produttiva e, pertanto, devono ritenersi relativi a quest'ultima, materialmente immedesimata nelle persone che sono preposte alle singole funzioni: le attrezzature, comprese quelle informatiche, devono allora reputarsi direttamente correlate alla funzione del soggetto che nel frangente rappresenta l'impresa e, solo in via mediata, assegnate alla singola persona comunque fungibile nel rapporto col mezzo medesimo»[137].

Il Trib. Milano, con sentenza emessa il 15 maggio 2002 ha così disposto: «*…. la "personalità" dell'indirizzo non significa necessariamente "privatezza" …. l'indirizzo aziendale, proprio perché tale, può sempre essere nella disponibilità di accesso e lettura da parte di persone diverse dall'utilizzatore consuetudinario (ma sempre appartenenti all'azienda). …..*

Così come non può configurarsi un diritto del lavoratore ad accedere in via esclusiva al computer aziendale, parimenti è inconfigurabile in astratto, salve

[137] Tribunale di Torino, 15 settembre 2006, sentenza n. 143, cit.

eccezioni di cui sopra, un diritto all'utilizzo esclusivo di una casella di posta elettronica aziendale.

Con sentenza n.13057 del 31 marzo 2016, la Corte di Cass. penale ha affrontato la questione relativa agli accessi di un dipendente pubblico alla posta elettronica, protetta da password, in uso da parte di un collega, a lui subordinato. Durante tale accesso, il superiore aveva visionato e scaricato alcuni documenti.

La Corte adita ha ritenuto che la protezione della mail con una password ha un significato evidente, ovvero rivela la volontà dell'utente di farne uno spazio riservato, pertanto ogni accesso rileva un'ipotesi di reato ex articolo 615 ter del c.p.[138]. La circostanza che l'accesso sia avvenuto in un sistema informatico pubblico, ha continuato la Corte, non attenua la gravità del reato, in quanto non si esclude che la mail possa rappresentare il domicilio informatico proprio del dipendente.

Per tale ragione, un eventuale accesso abusivo da parte di chiunque (quindi, anche da parte del superiore gerarchico), integra il reato previsto dall'articolo 615 ter c.p.

Secondo i giudici: "*la casella rappresenta uno "spazio" a disposizione della persona, sicché la sua invasione costituisce lesione della riservatezza in quanto, a quella "casella" è collegato uno ius excludendi, di cui anche i superiori devono tenere conto*.

In base a tale assunto, la Corte ha respinto quanto avanzato dalla difesa del superiore, che pretendeva l'equiparazione della casella mail alla

[138] In tal caso si configura un'ipotesi di Accesso abusivo ad un sistema informatico o telematico.

"cassetta delle lettere", poiché quest'ultima non è destinata a ricevere e custodire informazioni e non rappresenta una "*espansione ideale dell'area di rispetto pertinente al soggetto interessato*", bensì un mero contenitore di elementi solo indirettamente riferibili alla persona.

Con sentenza n. 47096 del 19 dicembre 2007, la Cassazione ha, invece, stabilito che non integra il reato previsto dall'articolo 616 c.p.[139] la lettura della e-mail aziendale del dipendente da parte del suo superiore gerarchico (o del datore di lavoro), laddove sia stato previsto che i suddetti debbano essere messi a conoscenza della password dispositiva[140].

Nelle decisioni 18 marzo 2014, n. 6222 ,Cass. civ. 29 settembre 2005, n. 19053 e Cass. civ. 17 giugno 2011, n. 13353, la Suprema Corte ha stabilito che laddove l'azienda non abbia predisposto, o pubblicizzato, una *policy* aziendale che disciplini l'utilizzo degli strumenti informatici aziendali, il lavoratore dipendente può sempre eccepire di non avere ricevuto tali direttive relative alle modalità con cui il datore avrebbe potuto controllare tali strumenti in uso per esclusive finalità professionali.

L'azienda, infatti, è tenuto a chiarire se e come si riserva di effettuare controlli, seppur saltuari e occasionali, provvedendo ad indicare le motivazioni che li rendono necessari. In presenza di regolare *policy* il datore non può comunque richiedere il licenziamento del lavoratore se quest'ultimo abbia utilizzato, per scopi personali, gli strumenti di lavoro

[139] Violazione, sottrazione e soppressione di corrispondenza.

[140] Infatti, in tal caso, la corrispondenza elettronica può dirsi "chiusa" solo nei confronti dei soggetti che non siano legittimati all'accesso dei sistemi informatici di invio o ricezione dei singoli messaggi.

aziendali, tra cui la mail personale, se il contratto collettivo applicato dovesse prevedere per tali inadempimenti o infrazioni delle sanzioni di tipo conservativo, quali la multa o la sospensione dal lavoro.

In mancanza di tale limite, la Corte di Appello ha chiarito che sussiste, invece, ipotesi di giusta causa di licenziamento, integrando tale comportamento come una grave violazione degli obblighi contrattuali, se il lavoratore ha dedicato del tempo destinato al lavoro, a collegarsi ad Internet per scopi personali, utilizzando la rete telefonica aziendale[141].

Secondo il tribunale di Firenze, costituisce giusta causa di licenziamento l'operato di un lavoratore dipendente che, durante l' orario d'ufficio, impiegando il personal computer di un collega assente dal lavoro, divulghi informazioni aziendali riservate[142].

Inoltre, secondo la Corte di appello di Milano, deve considerarsi illegittimo il licenziamento inflitto a seguito della rilevazione del collegamento a siti internet non lavorativi senza aver provveduto a contestare il tempo sottratto alla prestazione lavorativa[143]. La Cassazione ha ritenuto legittimo il licenziamento di un lavoratore che, per fini personali, si era connesso ad internet con il computer aziendale, scaricando documenti con programmi scaricati dal web , violando,

---

[141] Corte d'appello Ancona 1/8/2003,in *Lav. Nella giur*. 2004, 135, con commento di Georgia Baschemi.

[142] Trib. Firenze 25/6/2004, Est. Bazzoffi, in*: D&L* 2005, con nota di Filippo Pirelli, "Utilizzo fraudolento di strumenti informatici e licenziamento", 245.

[143] Corte app. Milano 30/9/2005, in: *D&L,* 2006, con nota di Stfano Chiusolo, "Abuso di internet e licenziamento: la Corte d'Appello di Milano passa in rassegna i molteplici profili di illegittimità", 899.

contestualmente, sia il regolamento di policy aziendale sia il codice disciplinare del contratto collettivo applicato dall'azienda[144].

Non giustifica, invece, il licenziamento del lavoratore l'installazione di un programma per scaricare musica sul pc aziendale [145].

Il tenore delle sentenze si colloca in seno al perimetro normativo che prevede che se non vi sia stata alcun accordo sindacale o con l'Ispettorato del Lavoro, si ritiene contrario all'art. 4 S. L. l'eventuale licenziamento basato su monitoraggio informatico.

In tali casi, infatti, si prefigurano ipotesi di trattamento dei dati sensibili ex artt. 1, 2° comma, lett. b e 22, 1° comma, L. 31/12/96 n. 675, - ora art. 4 lett. a) e di ricavare informazioni su fatti estranei alla sfera riguardante l'attitudine professionale, in violazione dell'art. 8 S.L.[146].

La sentenza Cass. n. 2056/2011 ha, invece, accolto favorevolmente il licenziamento intimato ad un lavoratore dipendente che, ad una persona estranea all'azienda, aveva consentito l'accesso alla postazione informatica personale,e di cui possedeva una password, esponendo l'azienda alla sottrazione di dati riservati.

Con la sentenza del 15 giugno 2017 n. 14862, la Cass. ha stabilito legittimo il licenziamento di un dipendente che 'abusa' della connessione internet aziendale.

Nel caso in oggetto, la Suprema Corte ha ritenuto legittimo il provvedimento citato poiché il comportamento era risultato intenzionale

---

[144] **Cass.**, Sez. L civile **Sentenza** 11/08/**2014**, **n**. **17859, in: www.dottrinalavoro.it.**

[145] Cass., sez. Lavoro, 26 novembre 2013, n. 26397, in:www.dottrinalavoro.it

[146] Corte app. Milano 30/9/2005, Pres. Castellini Est. Trogni, in D&L 2006, con nota di Stfano Chiusolo

e reiterato nel tempo. L'azienda aveva infatti rilevato ben 27 connessioni, che corrispondevano a circa 45 ore di traffico internet attuato in soli 60 giorni[147].

In questa vicenda, la mancata diffusione di un codice disciplinare sulle modalità di utilizzo dei computer aziendali ha rappresentato l'argomento principe con il quale il dipendente ha cercato di difendersi. Tale *policy* dell'azienda risponde sostanzialmente a tre esigenze: anzitutto stabilisce la disciplina dei comportamenti che il lavoratore può tenere nell'utilizzo dei *device* aziendali; in secondo luogo consente di orientare il convincimento giudiziale , riducendo il grado di incertezza legato ad un lungo e faticoso contenzioso e, infine,determina un effetto deterrente per il lavoratore.

Tuttavia, nel caso di specie, il dipendente, ad avviso della Corte, non ha rispettato i più generali doveri di diligenza e di fedeltà, disciplinati già nel codice civile, tra cui l'etica ed il buon senso comune.

La verifica da parte del datore di lavoro del rispetto di tali principi generali, non implica necessariamente, ad avviso della Corte, l'applicazione della specifica disciplina prevista dall'art. 4 dello Statuto dei Lavoratori che, unitamente al Codice della privacy, disciplina le modalità di controllo a distanza dei lavoratori e l'utilizzo delle informazioni ottenute. Infatti tali misure non si estendono alle condotte illecite dei lavoratori suscettibili a compromettere l'integrità del patrimonio aziendale, nonché il funzionamento degli impianti e la loro sicurezza. Infatti, se da un lato esiste un diritto del lavoratore alla

[147] Tali aspetti vennero rilevati utilizzando file log.

riservatezza nello svolgimento della prestazione, dall'altro è pur sempre richiesta diligenza dal datore di lavoro ai fini di un'efficiente e produttiva attività aziendale. Molte sono le sentenze che rimandano ad una conclusione condivisa ovvero che, pur rappresentando una forma di controllo a distanza lesivo dei diritti dei dipendenti, l'accesso da parte del datore di lavoro all'account aziendale, utilizzato dal dipendente, può ritenersi ammissibile se inquadrabile come modalità di "controllo difensivo". In tal senso, la Cass., sez. lav., 23 febbraio 2012, n. 2722, relativamente ad un cd. controllo a posteriori su un impiegato bancario che, con messaggi elettronici diretti a soggetti esterni all'istituto, aveva divulgato notizie riservate riguardanti un cliente correntista, ha stabilito che: «*tale fattispecie è estranea al campo di applicazione dell'articolo 4 dello statuto dei lavoratori. Nel caso di specie, infatti, il datore di lavoro ha posto in essere una attività di controllo sulle strutture informatiche aziendali che prescindeva dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa degli addetti ed era, invece, diretta ad accertare la perpetuazione di eventuali comportamenti illeciti (poi effettivamente riscontrati) dagli stessi posti in essere. Il cd. controllo difensivo…… era destinato ad accertare un comportamento che poneva in pericolo la stessa immagine dell'istituto bancario presso terzi*»[148].

In merito al tema dell'entità della sanzione, la Cass. il 18 marzo 2014, ha ritenuto che «*il datore di lavoro non può irrogare un licenziamento per giusta*

[148] L"attività di controllo sulle strutture informatiche aziendali da parte della banca- ha osservato la Cassazione- "*prescindeva dalla pura e semplice sorveglianza sull"esecuzione della prestazione*", essendo, invece, "*diretta ad accertare la perpetrazione di eventuali comportamenti illeciti (poi effettivamente riscontrati)*".

causa se trattasi di una sanzione più grave di quella prevista dal contratto collettivo applicabile in relazione ad una determinata infrazione»**.**

Con la successiva del 2 novembre 2015, n. 22353, la Cassazione ha statuito che nonostante l'abuso di chi utilizzi il personal computer in dotazione, la linea internet e la mail aziendale per scopi personali, il datore di lavoro deve rispettare la proporzione tra sanzione ed illecito disciplinare[149].

Secondo la Cass. è necessario che l'utilizzo personale della mail, e la navigazione in internet, non abbiano determinato una significativa sottrazione di tempo all'attività di lavoro, né un blocco del lavoro, con grave danno per l'attività produttiva.

Secondo i giudici,nei casi meno gravi, esiste liceità dell'irrogazione di sole sanzioni disciplinari più miti di natura conservativa (sospensione, multa, ecc.).

3.2 La sentenza CEDU 5 settembre 2017 (ric. n.61496-09)

La 4 sezione della Corte europea dei diritti umani, in data 12 gennaio 2016, stabilì che il datore di lavoro è legittimato a controllare le e-mail inviate e ricevute dai propri dipendenti e a licenziarli in caso di utilizzo dell'account aziendale per fini privati, in spregio alla *policy* aziendale[150].

Il caso specifico riguardava un datore di lavoro che, al fine di controllare l'effettiva attività svolta dal suo dipendente, aveva monitorato le sue

[149] **Cass.**, sez. Lavoro, sentenza del **2 novembre 2015**, **n°22353** , in Riv.Giur. del lavoro (RGL).

[150] La policy aziendale ne impone, invece, l'uso ai soli fini aziendali.

conversazioni *chat* e, fra esse, aveva rinvenuto la presenza di alcuni messaggi personali inviati dal lavoratore ad alcuni suoi parenti.

I giudici, inoltre, hanno ritenuto legittimo il controllo dell'account di posta aziendale da parte del datore, non rappresentando una violazione della sua *privacy*, in quanto la lettura delle comunicazioni telematiche rappresentava l'unico strumento a disposizione dell'azienda per verificare la responsabilità disciplinare del proprio dipendente.

La legittimazione al controllo aziendale è stata fatta discendere dalla fondata considerazione che l'*account* aziendale, pur essendo utilizzato dal lavoratore, risultasse, comunque, uno strumento aziendale di proprietà del datore di lavoro che poteva accedervi per eventuali controlli difensivi.

Tale sentenza ha rappresentato un riferimento fino al 2017, quando la Corte Europea dei Diritti dell'uomo ha completamente ribaltato la propria posizione fino ad allora assunta in tema di monitoraggio delle comunicazioni telematiche dei lavoratori dipendenti.

A seguito di ricorso del lavoratore, il 5 settembre 2017, con pronuncia n. 61496/2008, la Grande Camera della CEDU ha disconosciuto la sentenza del 2016, precisando che, affinché l'accesso del datore di lavoro alla mail aziendale potesse ritenersi legittimo, occorre avvisare il lavoratore sia sulla possibilità di essere monitorati che sulle modalità.

Il licenziamento disciplinare intimato al lavoratore si basava sul fatto che egli avesse utilizzato la connessione ad internet con finalità personali, scambiando messaggi durante le ore lavorative con il fratello e la fidanzata tramite l'account Yahoo attivato originariamente dal soggetto al

solo fine di gestire le relazioni con i clienti. Dopo aver monitorato le sue mail ed aver avuto prova che il contenuto delle stesse avessero tutt'altro che carattere professionale, l'azienda ha contestato al lavoratore la violazione del suo regolamento interno e la conseguente riduzione della produttività. Si ribadiva, inoltre, che allatto dell'assunzione, era stato mostrato un documento aziendale che informava circa il divieto di utilizzare i beni aziendali per fini personali, pena il licenziamento.
Il ripensamento della Corte si è basato sulla constatazione che, il paese in cui aveva sede l'azienda, la Romania, aveva violato l'articolo 8 della CEDU, in quanto incapace di garantire il rispetto della riservatezza di un suo cittadino**.**

3.3 Casi specifici. I principali Provvedimenti emanati dal Garante per la privacy

Il Garante per la *privacy* ha, a più riprese, divulgato una serie di principi dettati per evitare l'uso improprio degli strumenti telematici forniti ai dipendenti. Fra tali principi, si ricordano i seguenti:
a) impiegare filtri per prevenire determinate operazioni, quali l'accesso a siti inseriti in *black list* od il *download* di file musicali o multimediali;
b) individuare preventivamente i siti considerati correlati o meno con la prestazione lavorativa;

c) utilizzare indirizzi e-mail condivisi tra più lavoratori (es. urp@ente.it; info@ente.it; ufficioreclami@ente.it), rendendo così chiara la natura non privata della corrispondenza;

d) attribuire ai dipendenti anche una e-mail ad uso personale;

f) introdurre procedure per consentire al dipendente di delegare un suo fiduciario per verificare i messaggi a lui indirizzati in caso di sua assenza;

g) l'utilizzo di messaggi di risposta automatica nel caso di assenza del dipendente.

Oltre a tali principi, il Garante ha provveduto ad emanare, varie delibere volte ad individuare linee guida per l'utilizzo di internet e della posta elettronica,tra cui rileva quella emessa nel 2007[151].

Secondo la delibera citata, i *log file* di traffico *e-mail* e l'archiviazione di messaggi si traducono in controlli che, per essere conformi alla normativa in materia di protezione dei dati personali e alle regole di settore sul rapporto di lavoro, richiedono al datore di informare i lavoratori preventivamente della possibilità di essere monitorati.

Inoltre, il Garante chiarisce che, nell'effettuare i controlli circa il corretto utilizzo degli strumenti di lavoro, occorre riferirsi a quanto previsto dagli artt. 2086, 2087 e 2104 c.c., nel rispetto della libertà e dignità dei lavoratori.

In merito alle strumentazioni *hardware* e *software* impiegabili per il controllo dell'utente di un sistema di comunicazione elettronica , il provvedimento in oggetto ha chiarito che esse rientrano nel divieto di

[151] Provvedimento emesso il ° marzo 2007, n. 13, in:*www.garanteprivacy.it*

installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* (*art. 4, 1° co., L. n. 300/1970*).

Il Provvedimento 22 dicembre 2016 n.547 ha visto invece, il Garante per la privacy ritenere essere in contrasto con la disciplina dei controlli a distanza "*la raccolta sistematica delle comunicazioni elettroniche in transito sugli account aziendali dei dipendenti in servizio, la loro memorizzazione per un periodo di dieci anni e la possibilità di accedervi all'esito di una procedura di Security Investigation Request consente alla società di effettuare il controllo dell'attività dei dipendenti*[152]".

Nel Provvedimento 13 luglio 2016, n. 303[153] l'Authority ha considerato illegittimo il monitoraggio massivo delle attività in internet dei dipendenti di un'università[154] che aveva conservato, per 5 anni, i *file di log* sul traffico internet, dall'utilizzo delle mail alle connessioni di rete.

I dati erano riconducibili ai singoli utenti, grazie agli indirizzi IP (indirizzo internet) e ai *Mac Address* (identificativo *hardware*) dei pc.

Inoltre, tali limitazioni dipendono dalla circostanza per cui, il *software* di controllo non possono ritenersi "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa". Infine, si eccepì che l'Università non aveva fornito alcuna informativa sulla privacy, violando così il principio di liceità, posto alla base del trattamento dei dati personali.

---

[152] Cfr. artt. 11, comma 1, lett. a) e 114 del Codice e art. 4, legge 20.5.1970, n. 300). Tale disciplina infatti, pure a seguito delle modifiche disposte con l'art. 23 del decreto legislativo 14 settembre 2015, n. 151, non consente l'effettuazione di attività idonee a realizzare (anche indirettamente) il controllo massivo, prolungato e indiscriminato dell'attività del lavoratore".

[153] In : *www.garanteprivacy.it*

[154] Fra cui docenti, ricercatori, personale tecnico amministrativo e bibliotecario, studenti, dottorandi, specializzandi e assegnisti di ricerca.

Con un successivo Provvedimento, emanato il 30 luglio 2015, n. 456, l'Authority,nel sottolineare l'onere del datore di lavoro di informare i lavoratori preventivamente sull'eventuale effettuazione di controlli, ha evidenziato la necessità di un disciplinare sulla conservazione dei file di *log* relativi alle mail in transito sugli *account* aziendali.

Con riferimento ai trattamenti della posta elettronica aziendale dopo la cessazione del rapporto di lavoro, il provvedimento chiarisce che, in questi casi, gli *account* riconducibili a persone identificate o identificabili, devono essere rimossi. Con i Provvedimenti datati 18 ottobre 2012, n. 307 e 7 aprile 2011, n. 139, il Garante ha disposto il divieto di effettuare, con cadenza regolare, operazioni di *backup* sulle cartelle dei dipendenti.

Con il Provvedimento emesso dal garante per la *privacy* il 24 febbraio 2010 si è ritenuto che, pur riconoscendo il diritto del datore ad acquisire prova dell'utilizzo non consentito della rete, la verifica tramite visione dei contenuti del disco fisso costituisce un trattamento di dati eccedente rispetto alle finalità perseguite.

Proprio con tale logica, il Garante per la *privacy* aveva bloccato una verifica sul disco fisso del *computer* dalla quale era emersa la visione di materiale pornografico[155].

Sempre nel 2010, l'Autorità precisò che fosse opportuno che il datore adottasse tutte le misure utili a prevenire controlli successivi sul lavoratore[156]. Infine, il Provvedimento 2 aprile 2008, ha visto il Garante considerare illecita l'estrazione dall'*account*, della mail di un lavoratore

[155] Provvedimento 10 giugno 2010, n. 218, in:*www.granteprivacy.it*

[156] Quali l'individuazione di categorie di siti correlati o meno con la prestazione lavorativa, la configurazione di sistemi o l'utilizzo di filtri che prevengono determinate operazioni reputate incoerenti i con l'attività lavorativa.

dipendente attuata da parte di investigatori al fine di verificare l'operato di alcuni dirigenti.

Il Garante per la *privacy* ha ritenuto illecito il trattamento nel caso specifico,in quanto non era stato stipulato alcun accordo sindacale, né era stata ottenuta un'autorizzazione amministrativa ai sensi dell'art. 4, co. 2, S. L.

Conclusioni

Alla luce di quanto esposto è possibile stabilire l'esistenza di alcuni punti fissi che rivelano la versatilità della natura del rapporto tra datore del lavoro e lavoratore dipendente, configurandone gli aspetti di collaborazione, imprescindibili per il raggiungimento dello scopo comune e, al contempo, la necessità di evitare che la discrezionalità operativa attribuita al lavoratore assuma connotati di autarchia.

Il datore di lavoro ha il diritto di orientare l'attività, secondo le esigenze perseguite, nel rispetto della dignità e della *privacy* del lavoratore.

Nell'ottica appena descritta, rientra il tema dell'uso di internet e della mail aziendale, da parte del lavoratore dipendente.

Essendo giuridicamente riconosciuta un'equiparazione fra comunicazioni di natura telematica e corrispondenza, le e-mail e le comunicazioni via chat sono garantite dall'art. 15 della Cost. che ne tutela, tra l'altro, la libertà e la segretezza.

Oltre alla Costituzione, i controlli del datore di lavoro sulle attività dei lavoratori a lui subordinati vengono disciplinati da altre fonti. In base all'art. 4 Stat. Lav. si possono configurare tre diverse macro aree di controllo del datore di lavoro sull'attività svolta dai dipendenti:la prima riguarda i *controlli assolutamente illeciti* inibiti in quanto rispondono unicamente all'esigenza di controllare le operazioni svolte, pur in mancanza di reali istanze tecniche.

Una seconda classe di controlli riguarda i monitoraggi *ammissibili, ma condizionati* al preventivo accordo sindacale, ovvero all'autorizzazione dell'Ispettorato nazionale del lavoro[157] .

In questo caso, l'art. 4 Stat. Lav. tutela le contestuali esigenze di salvaguardia della dignità del lavoratore e di preservazione del patrimonio aziendale, inteso anche nella sua accezione intangibile, di *know how* e 'sapere' generico.

Tuttavia, da un punto di vista squisitamente tecnico, potenzialmente tale controllo nel monitorare le prestazioni, perviene ad informazioni personali sul lavoratore, evidenti nelle navigazioni effettuate oppure nei contenuti delle mail inviate o ricevute. Tutto ciò connota un'invasività dell'azienda nella sfera personale del lavoratore.

Il legislatore ha optato per una polifunzionalità delle apparecchiature, ammissibili in quanto funzionale alle esigenze organizzative, produttive, di sicurezza sul lavoro e di tutela del patrimonio aziendale.

È occorsa, in tale ottica, una soluzione che assicurasse la contestuale soddisfazione delle due esigenze, quella del datore, che consiste nell'assicurarsi che il tempo retribuito venga destinato all'attività e quello del lavoratore di difendere la propria *privacy*. A tale scopo la necessità di predisporre un piano di *policy* aziendale che indichi le modalità ed i tempi con cui attivare il monitoraggio.

La terza forma di monitoraggio concerne i *controlli pienamente legittimi* e *non condizionati*, vale a dire: *a) le verifiche attuate mediante strumenti di consueta utilità aziendale,* quali, ad es., l'accesso (condiviso dai dipendenti e

[157] Art. 4, co. 2, Stat. Lav., come mod. dall'art. 5, co. 2, D. Lgs. 24 settembre 2016, n. 185.

dall'impresa) all'archivio informatico; la sorveglianza sulla persona attuata, anche in modo occulto, da investigatori privati, senza l'uso di strumentazioni a distanza; c) i c.d. 'controlli difensivi', categoria elaborata in sede giurisprudenziale in vigenza del vecchio testo dell'art. 4 Stat. Lav., ove il controllo datoriale non ha ad oggetto l'attività lavorativa propriamente detta ed è giustificato dal fine di tutela del patrimonio aziendale rispetto agli illeciti civili e penali dei dipendenti; d) la rilevazione a distanza degli accessi di presenza (i c.d. badge marca-tempo); e) gli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" con i quali è possibile oggi effettuare controlli a distanza senza esperire preventivamente la procedura codeterminativa con il sindacato ovvero, in caso di mancato accordo, la procedura in sede amministrativa. (ad es., computer, cellulare, *tablet*).

Mentre lo Statuto dei lavoratori disciplina il controllo a distanza generico, esistono altre norme che regolano in maniera specifica l'accesso alle mail aziendali. In *primis* è necessario riferirsi al tenore del D. Lgs. 196/2003, che regola la protezione dei dati personali e che stabilisce che, i dipendenti devono essere informati circa l'esistenza, le finalità e le caratteristiche del trattamento dei loro dati, in ottemperanza agli obblighi posti al titolare.

Anche l'UE si è espressa sull'argomento con la Direttiva 46 del 1995 che ha istituito il Gruppo di lavoro art. 29 (WP29), formato da esperti sul tema, che ha stabilito che ogni lavoratore, indipendentemente dal tipo di contratto a lui applicato, ha diritto al rispetto della vita privata, della sua libertà e dignità, pertanto deve essere informato circa le modalità di trattamento dei dati personali.

Il Gruppo ha raccomandato l'adozione di misure preventive volte alla protezione della riservatezza dei lavoratori redigendo, se del caso, anche una valutazione precisa dell'impatto generale del trattamento, avendo cura di rilevare i dati in modo da contemperare sia quanto necessario per il legittimo interesse aziendale, sia quanto ammesso dall'uso delle nuove tecnologie informatiche (*principio del bilanciamento*).

Il Regolamento n. 2016/679, entrato in vigore nel settembre 2018, ha completamente sostituito la Dir. 46/95 e, con essa, il Codice della *privacy*.

Il Regolamento in oggetto esorta l'intervento per favorire la trasparenza del trattamento, il trasferimento di dati personali all'interno delle unità produttive o di un gruppo di imprese che svolge una comune attività e l'adozione di sistemi di monitoraggio sul posto di lavoro. Inoltre, è stato confermato quanto già stabilito nel Codice della privacy che prevede che ciascun lavoratore debba essere informato circa le modalità di trattamento dei propri dati personali.

Il Regolamento ha, infine, previsto che il datore di lavoro sia tenuto anche ad adottare specifiche misure di sicurezz**a** per prevenire violazioni della riservatezza degli interessati, tra cui:

- il divieto di monitoraggio delle cartelle/dei file e/o delle comunicazioni personali dei dipendenti;
- l'esclusione delle cd. "aree sensibili" dalle zone sottoposte a monitoraggio;

la previsione di un monitoraggio "a campione", rispetto ad una sorveglianza continuata nel tempo.

Sul tema del controllo dell'uso dei *computers* da parte dei lavoratori, un particolare rilievo è dato dal tenore del D. Lgs. n. 151/2015 (c.d. Jobs Act) che, modificando l'art. 4 dello Statuto dei lavoratori, pur conservando il divieto dei controlli a distanza, ha consentito la loro utilizzazione in caso di accordo sindacale o un' autorizzazione ministeriale.

Rispetto al passato, il Jobs Act ha reso più flessibile l'adozione di misure di controllo dei lacvoratori prevedendo che, in linea generale, tali autorizzazioni dovranno essere sempre concesse in caso di commissione di illeciti che ledono l'immagine o il patrimonio dell'azienda.

Il controllo dell'uso di internet da parte dei lavoratori è stato oggetto di reiterati interventi da parte dell'Authority garante per la *privacy* che ha fornito importanti linee guida sul tema.

L'*Authority*, ha suggerito, in particolare, l'adozione di alcuni principi: *a) il "principio di necessità", che prevede che i programmi informatici ed i sistemi informativi debbano essere configurati riducendo al minimo l'impiego dei dati personali ed identificativi in relazione alle finalità perseguite;*

b) *il "principio di correttezza", secondo cui le modalità dei trattamenti devono essere rese note ai lavoratori;*

c) il "principio di pertinenza e non eccedenza", per cui le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" ed il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile.

Il Garante, inoltre, propone di introdurre in azienda un disciplinare interno in cui chiarire i limiti relativi all'uso di internet e della posta elettronica, specificando precisi aspetti, quali :

i comportamenti ritenuti tollerati rispetto alla "navigazione" in Internet (ad es., il *download* di *software* o di *file* musicali) e in quale misura è consentito l'impiego per ragioni personali di servizi di posta elettronica o di rete.

Il Garante suggerisce di indicare, eventualmente, una postazione di *computer* da cui è concesso l'accesso alla rete, indicandone le modalità e l'arco temporale di utilizzo, durante la giornata lavorativa.

In considerazione della possibilità dell'azienda di tracciare i collegamenti ad internet tramite *file di log* o semplici *back up* è suggerito di informare i lavoratori circa le informazioni memorizzate.

Infine, il Garante, consiglia di indicare se, e in quale misura, il datore di lavoro si riserva di effettuare controlli e le relative modalità con cui verrebbero effettuati e le conseguenze, anche di tipo disciplinare, sul lavoratore inadempiente.

La mancata esplicitazione di una *policy aziendale* ha effetti sostanziali nelle eventualità di uso improprio di internet da parte del lavoratore.

In assenza di una predisposizione di una *policy* aziendale si può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione trasformando in legittimi alcuni usi impropri della posta elettronica.

In tal senso si sono espresse diverse pronunce giurisprudenziali.

In pratica, il datore non può difendersi con successo in un giudizio sul merito del controllo dell'uso di internet, laddove non ha preventivamente predisposto e comunicato la policy di monitoraggio.

Anche la 4° sezione della Corte europea dei diritti umani, in data 12 gennaio 2016, stabilì che il datore di lavoro è legittimato a controllare le e-mail inviate e ricevute dai propri dipendenti e a licenziarli in caso di utilizzo per fini privati, in spregio alla *policy* aziendale, successivamente, però, ha rivisto tale orientamento, stabilendo che occorre prima informare i lavoratori circa le modalità ed i tempi di monitoraggio.

Tuttavia, occorre chiarire che l'orientamento dei giudici, non ha trascurato il tipo di utilizzo di internet e delle mail effettuato, anche in assenza della policy.

In tal senso, la Cass., sez. lav., 23 febbraio 2012, n. 2722, relativamente ad un cd. controllo a posteriori su un impiegato bancario che, con messaggi elettronici diretti a soggetti esterni all'istituto, aveva divulgato notizie riservate riguardanti un cliente correntista, ha stabilito che: *«tale fattispecie è estranea al campo di applicazione dell'articolo 4 dello statuto dei lavoratori. Nel caso di specie, infatti, il datore di lavoro ha posto in essere una attività di controllo sulle strutture informatiche aziendali che prescindeva dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa degli addetti ed era, invece, diretta ad accertare la perpetuazione di eventuali comportamenti illeciti (poi effettivamente riscontrati) dagli stessi posti in essere. Il cd. controllo difensivo…… era destinato ad accertare un comportamento che poneva in pericolo la stessa immagine dell'istituto bancario presso terzi».*

Il Garante per la *privacy* ha, infine,suggerito l'adozione di un doppio binario di mail, ad uso personale ed aziendale, precisando, nel documento di *policy,* gli impieghi consentiti ed indicando alcuni indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.).

Bibliografia

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.

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

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

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

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

BARTOLE S. , DE SENA P. , ZAGREBELSKY V., *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, CEDAM, 2012.

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

CARINCI F., *Rivoluzione tecnologica e diritto del lavoro, in Giornale di diritto del lavoro e delle relazioni industriali*, 1985

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

CASTELLANETE A., *Notizie e commenti sul diritto interazione e dell'Unione europea*, 299 http://www.marinacastellaneta.it/blog/controllo-delle-mail-aziendali-da-parte-deldatore-di-lavoro-compatibili-con-la-cedu.html.

COMMISSARIATO DI P.S. online, Approfondimenti Cyberstalking, in :http://www.commissariatodips.it/approfondimenti/cyberstalking.html

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

DE GIORGI M., *La tutela della privacy per il consumatore in rete, in La privacy in Internet*, a cura di A. LISI, Ed. Simone, 2003.

DE GRAZIA L.M., *In Internet ed Intranet, sicurezza e privacy: i pericoli nascosti nell'applicazione della l. 675/96 e del d.lgs. 318/99* in: "*Furto di identità ovvero frode da impersonificazione: Cosa è? Quali sono i rischi? quanto è diffuso? come difendersi*?", 2013, in *www. Europeanprivacycentre.eu.*

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*?, in: *Diritto e giustizia*, 2015.

DI MARTINO C. e VOLTAN E.F., *Diritto alla privacy per le imprese ed i professionisti*, 2006.

FABRIS F., *Il diritto alla privacy tra passato, presente e futuro*, in *Rivista di scienze della comunicazione*, 2009, n. 2.

FORTUNA F.S., *I reati in materia di lavoro, Trattato di diritto penale dell'impresa*, vol. VIII, CEDAM, 2002. In: *Giurisprudenza ex multis* Cass. Pen., Sez. IV, 22.03.1985 in *Giust. Pen*., 1986, II.

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

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/-/docwebdisplay/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/-/docce display/docweb/1819504.

GENTILINI G.*, Cenni sulla responsabilità derivante dall'esercizio di attività pericolose con specifico riguardo alle fonti di elettromagnetismo*., Dicembre 2001, in:*www.diritto.it.*

GIUGNI G., *Diritto sindacale*, Bari, 2010. A cura di BELLARDI, CURZIO e GAROFOLO

IAQUINTA F., INGRAO A., *Il datore di lavoro e l'inganno di Facebook,* in: *Rivista Italiana di Diritto del Lavoro*, 2014

LAMBERTUCCI P., *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a distanza tra attualità della disciplina statutaria,*

promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs Act), in WP CSDLE "Massimo D'Antona", 235/2015.

LAMBERTUCCI P., *Svolgimento del rapporto di lavoro e tutela dei dati personali*, in AA.VV. *La tutela della privacy del lavoratore*, UTET, 2001.

LEVI A., *Il controllo informatico sull'attività del lavoratore*, Torino, Giappichelli, 2013

MARAZZA M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE "Massimo D'Antona".I T – 300/2016, Roma, 2016.

MARCHESI G., *Mail aziendale e messaggi privati: la sentenza CEDU*, in: *Glob.Press*, 2016

MARESCA A., C*ontrolli 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.

MC CLURE S., SCAMBRAY J., KURTZ G., Hacker! 7.0 *Nuove tecniche di protezione*, Milano, Apogeo editore, 2013.

MINERVINI A., *I controlli sul lavoratore e la tutela dell'azienda*, in La giurisprudenza nel lavoro, Milano 4/2014.

MINISTERO DELLO SVILUPPO ECONOMICO, Piano nazionale Industria 4.0, in http://www.sviluppoeconomico.gov.it/index.php/it/industria

MODESTI A., *Il controllo a distanza del lavoratore tra il diritto alla riservatezza e la tutela del patrimonio aziendale*, Roma, *Ragiusan* n. 369/370, 2015.

MONDUCCI J., *Controllo del lavoratore e trattamento dei dati personali*, in: *Diritto e Pratica delle Società*, 2, luglio 2001, Il Sole 24 Ore.

NATALI P. J., *Navigazione Internet dei lavoratori e tutela della privacy*, in: *Diritto & Pratica del Lavoro*, 32-33/2015.

PARODI C., *VoIP, Skype e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle comunicazion*i?, in *Diritto penale e processo*, 2008, 1309.

PERSIANI M., *Fondamenti di diritto del lavoro*, Padova, 2015.

PERSIANI M., *Fondamenti di diritto del lavoro*, seconda edizione, Padova, Cedam, 2015.

PERULLI A., *Il potere direttivo dell'imprenditore*, Milano, Giuffè, 1992.

PESSI R., *Lezioni di diritto del lavoro*, quarta edizione, Torino, Giappichelli, 2012.

PIZZETTI F. , *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016.

POLICELLA O., *Controlli dei dipendenti: gli impianti audiovisivi nel nuovo art. 4 dello Statuto dei lavoratori*, 2015, http:// www.diritto24.ilsole24ore.com.

RAIMONDI F., *La riservatezza del lavoratore tra innovazioni legislative e giurisprudenza nazionale ed europea*, in: *Rivista giuridica del lavoro*, 2/2016.

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., *Intervista su privacy e libertà*, Bari, Laterza, 2005.

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

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.

SALAZAR P., *Facebook e rapporto di lavoro: a che punto siamo, in il Lavoro nella giurisprudenza*, 2/2016.

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.

SANTONI F., *Controlli difensivi e tutela della privacy dei lavoratori*, in *Giur. italiana*, 2016.

SANTONI F., *Controlli difensivi e tutela della privacy dei lavoratori*, in: *Giurisprudenza italiana*, 2016.

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

SCIUMBATA G., *I reati societari*, Giuffrè, 2002.

SERVIDIO S., *Controllo dei dipendenti e difesa del patrimonio aziendale*, in: Diritto & Pratica del Lavoro, 12/2016.

SITZIA A., *I controlli a distanza dopo il "Jobs Act" e la raccomandazione* R(2015) del Consiglio d'Europa, Legge e giustizia, in il Lavoro nella giurisprudenza, 7/2015.

SITZIA A., *Il controllo (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., *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali,* Padova, CEDAM, 2013.

SORO A., *Liberi e connessi*, Torino, Codice edizioni, 2016.

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

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

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

SUTTI S., *La sicurezza dei sistemi informativi aziendali, norme protettive, oneri e misure obbligatorie, in La privacy in Internet*, a cura di A. LISI, Ed. Simone, 2003

TEA A., *Controlli a distanza:spunti problematici e sviluppi interpretativi*, in: *Il Lavoro nella giurisprudenza*., 1/2017

TROJSI A., *Il comma 7, lettera f) della legge delega n. 183/2014. Tra costruzione del Diritto del lavoro dell'era tecnologica e liberalizzazione dei controlli a distanza sui lavoratori*, in M. Rusciano et al., *Jobs Act e contratti di lavoro dopo la legge delega 10 dicembre 2014*, n. 183, W.P. CSDL "Massimo D'Antona", http://csdle.lex.unict.it/, collective.

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

WESTIN A., *Privacy and Freedom*. New York: Atheneum,1967.

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