RIVISTA ITALIANA DI DIRITTO DEL LAVORO
ISSN 0393-2494
Anno XXXII Fasc. 2 - 2013

Filippo Olivelli

IL DIFFICILE BILANCIAMENTO TRA LA TUTELA DELLA *PRIVACY* E LE ESIGENZE DI CONTROLLO DEL DATORE DI LAVORO

Estratto

MVLTA PAVCIS AG

Milano • Giuffrè Editore

TRIBUNALE DI FERRARA 27 agosto 2012, n. 172 - De Curtis *Giud.* - Z.O. (avv. Lopez) c. Centro servizi degli A.T.C. Provincia di Ferrara (avv. Mazzanti).

Controlli a distanza - Corretto impiego del computer aziendale - Controllo occasionale - Violazione dei canoni di lealtà e correttezza.

Il controllo effettuato sul computer aziendale in uso al dipendente teso a verificare l'eventuale compimento di condotte illecite, svolto in maniera del tutto occasionale e dopo il sostanziale disinteresse del datore di lavoro in ordine all'adozione di misure tali dal assicurarne il corretto impiego, è da considerarsi illegittimo per violazione dell'art. 4, l. n. 300/1970 e art. 11, d.lgs. n. 196/2003, poiché tale comportamento integra la fattispecie di trattamento dei dati personali del lavoratore effettuato all'infuori dei canoni di lealtà e correttezza e non per scopi determinati, espliciti e legittimi. (1)

Svolgimento del processo. — 1. Con ricorso depositato in data 10 luglio 2007 Z.O., premesso di aver lavorato alle dipendenze della associazione convenuta (e sue precedenti formazioni) sin dal 1982 con mansioni di impiegato di 1° livello, presso la sede di Ferrara, e dopo aver illustrato la struttura e le funzioni del Centro Servizi rispetto agli A.T.C. (Ambiti Territoriali di Caccia) in essa consociati, — *Omissis* — esponeva: — *Omissis*

— che infatti il giorno 15 ottobre 2008, fissato per il tentativo di conciliazione innanzi alla D.P.L., la datrice di lavoro predisponeva una lettera di addebito disciplinare, pervenutagli il successivo 17 ottobre 2008, con la quale veniva contestato ad esso ricorrente che «a seguito di controlli casuali» disposti dalla Presidenza ed effettuati il 26 settembre 2008 da una ditta specializzata era emerso che il computer a lui assegnato e da lui abitualmente utilizzato presentava *software* non originale, non adeguato all'attività istituzionale e non autorizzato tra cui anche un programma per scaricare *files*, musica e filmati; nel computer venivano altresì rinvenute immagini a contenuto erotico provenienti da *internet* nonché *files* personali ed attinenti ad un'altra ditta (Casa di Riposo Villa Aurora) che nulla avevano a che vedere con l'attività istituzionale dell'associazione; — O*missis*.

— di avere sollecitato la controparte a provvedere in merito alla contestazione disciplinare il 4.12.2008 ed il 8.1.2009 e di avere ricevuto in risposta al secondo sollecito comunicazione con la quale veniva evidenziato che il provvedimento che definiva il procedimento con il licenziamento per giusta causa era stato adottato il 15 dicembre 2008 e risultava comunicato al dipendente a mezzo

(1) La nota di F. Olivelli segue il testo della sentenza.

telegramma ed a mezzo posta celere con avviso di ricevimento in data 18 dicembre 2008.

Tanto premesso, il ricorrente contestava l'atto di recesso sotto diversi profili con articolata esposizione in diritto. In particolare, affermava che il licenziamento: — *Omissis*.

5) Era illegittimo in quanto disposto in violazione degli artt. 4 ed 8 Statuto dei Lavoratori nonché Codice della *Privacy* di cui al d.lgs. n. 30 giugno 2003, n. 196, poiché il controllo sul computer concretava un cd. trattamento dei dati sensibili avvenuto di nascosto, violando la *password*, senza previa comunicazione all'interessato; il controllo era avvenuto in modo lesivo della dignità del lavoratore, in violazione dei principi di trasparenza, proporzionalità non discriminazione e non vessatorietà; egli era poi stato costretto a rendere giustificazioni innanzi a tutti i membri del Consiglio de del Collegio dei Revisori; pertanto i dati ricavati dall'illecito monitoraggio informatico dovevano considerarsi del tutto inutilizzabili per qualsivoglia finalità;

6) *Omissis*. — quanto agli altri *files* e *softwares* mai la datrice aveva in precedenza vietato ai propri dipendenti di accedere a linee *internet* e fare il *download* di programmi;

7) era comunque illegittimo in quanto costituente sanzione manifestamente sproporzionata rispetto al fatto contestato, in quanto l'elemento soggettivo della condotta era grandemente ridimensionato in ragione della tolleranza datoriale circa l'accesso alla rete *internet* e l'uso della strumentazione aziendale in genere ed in considerazione del fatto che esso ricorrente era privo di precedenti. — *Omissis*.

Motivi della decisione. — *Omissis*. — 6. Il controllo sul computer del ricorrente si configura come illegittimo trattamento dei dati personali.

Devono invece condividersi le asserzioni della parte ricorrente in merito alla illegittimità del licenziamento in quanto conseguente e connesso ad una illegittima acquisizione di dati personali.

Il controllo sui computer dell'associazione è stato attuato ad iniziativa individuale del Presidente del Centro Servizi, dott. G.M., il quale ritenendo «opportuno mettere in sicurezza i sistemi informatici in uso presso gli uffici sede del Centro Servizi», con lettera in data 23.9.2008 diretta alla B.S.B. Sistemi S.r.l., conferiva incarico alla stessa «di provvedere alla revisione dei computers controllando per ogni singola macchina: 1. L'originalità dei programmi installati; 2. La presenza di password; 3. L'esistenza di programmi non attinenti l'attività del Centro Servizi», autorizzando la ditta a fare copia del contenuto dei computers per provvedere al controllo commissionato e riferire con relazione sui punti sopra evidenziati. Il tutto con il dichiarato scopo «di non incorrere, in caso di controllo da parte delle competenti Autorità, a sanzioni civili e penali, che sarebbero conseguenti al mancato rispetto delle norme in campo informatico». Da quanto

emerge dal doc. 29 parte convenuta la ditta era stata anche incaricata di annullare e reimpostare la *password* del computer.

La B.S.B ha riferito per iscritto di avere constatato che nel computer si trovavano *software* non originali, l'installazione di un programma di *filesharing* per scaricare musica e film, la presenza di film ed immagini a contenuto erotico scaricati da *internet*, nonché documenti di videoscrittura e fogli elettronici contenenti dati ed informazioni non inerenti al Centro Servizi.

Ritiene questo giudicante che l'ampia verifica effettuata sul computer costituisca «trattamento dei dati personali» così come previsto e disciplinato dal d.lgs. n. 196/2003 (cd. Codice della *privacy*). L'art. 4 del decreto definisce il trattamento come «qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati». Definisce altresì il dato personale come «qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale».

Da quanto emerge dalla lettera di incarico sopra ricordata si è trattato di un controllo occasionale, ma esso non conseguiva a specifiche sospette attività illecite del dipendente, trattandosi semplicemente di una verifica volta ad accertare non meglio precisate norme nel settore informatico per evitare sanzioni civili e penali genericamente indicate. Né risultava minacciata in modo imminente la sicurezza del sistema informatico del Centro Servizi, non essendo nemmeno stata allegata e provata la circostanza.

Risulta invece provato che l'utilizzo dei computers era avvenuto per anni nel sostanziale disinteresse del datore di lavoro il quale aveva lasciato proprio allo Z. la gestione degli aspetti tecnici legati all'uso dei p.c. dell'ufficio — *Omissis*. Il controllo del computer è stato dunque improvviso, imprevisto e del tutto estemporaneo.

Non può dunque essere invocato, come invece fa la parte convenuta, il diritto di difesa allo scopo di evidenziare che il diritto alla *privacy* non è assoluto, non scorgendosi a quale necessità difensiva doveva far fronte l'associazione. Né il controllo può essere considerato lecito alla luce del fatto che *ex post* sia stata accertata la non liceità o la non correttezza della condotta del dipendente. Ché altrimenti molte intrusioni immotivate nei dati personali del lavoratore dipendente potrebbero in tal modo risultare legittimate all'esito dei controlli.

Analogamente, non può essere utilizzato l'argomento secondo cui il controllo era solo occasionale e non diretto a monitorare a distanza l'attività del dipendente; del pari non significativa la circostanza che esso sia avvenuto su tutti i computer in uso agli unici tre dipendenti. Trattasi infatti di circostanze insuffi-

cienti a giustificare il trattamento dei dati personali per le ragioni che seguono.

Secondo l'art. 11 del Codice della *privacy*, il trattamento dei dati personali deve infatti essere attuato «in modo lecito e secondo correttezza» e la raccolta in copia e registrazione dei medesimi sarebbe dovuta avvenire «per scopi determinati, espliciti e legittimi»; in caso di violazione di tali principi i dati trattati «non possono essere utilizzati».

Tali principi hanno trovato ulteriore specificazione nelle linee guida del Garante per la protezione dei dati personali, adottate con deliberazione n. 13 del 1.3.2007 pubblicate in Gazzetta Ufficiale n. 58 del 10.3.2007, in materia di utilizzo di posta elettronica e della rete *internet* nel posto di lavoro.

Il Garante muove dalla premessa che compete al datore di lavoro, titolare del trattamento dei dati personali, assicurare il corretto impiego di tali mezzi ed adottare idonee misure di sicurezza anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità; così come gli compete per tali ragioni il controllo dell'utilizzo di *internet* e della posta elettronica sino alla conoscenza del contenuto della corrispondenza. Il Garante precisa che le informazioni scaturenti da tali controlli costituiscono trattamento dei dati personali anche sensibili riguardanti lavoratori o terzi.

Egli ricorda i cogenti principi contenuti nel Codice della *privacy* che devono essere rispettati nel trattamento dei dati: «a) il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice, par. 5.2); b) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, co. 1, lett. *a* del Codice)». Le tecnologie dell'informazione (in modo più marcato risetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (v. par. 3, c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime (art. 11, co. 1, lett. *b*, del Codice: par. 4 e 5), osservando il principio di pertinenza e non eccedenza (par. 6). Il datore di lavoro deve trattare i dati «nella misura meno invasiva possibile»; le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8) ed essere «mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza» (Parere n. 8/2001, cit., punti 5 e 12).

Di qui consegue la considerazione che, poiché il trattamento deve ispirarsi al canone della trasparenza (v. art. 4 Statuto dei lavoratori e par. 3, d.lgs. n. 626/1994), il datore di lavoro ha l'onere di indicare caso per caso, chiaramente ed in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati i controlli. «Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando

il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio di piccole realtà dove vi è una continua condivisone interpersonale di risorse informative».

Il Garante osserva che dovrebbe essere tra l'altro specificato se ed in quale misura il datore di lavoro si riserva di effettuare controlli, anche saltuari od occasionali, indicando le ragioni legittime — specifiche e non generiche — per cui verrebbero effettuati e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni) e quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete *internet* sono utilizzate indebitamente.

Con particolare riferimento alla navigazione nella rete *internet*, secondo il Garante «il datore di lavoro, per ridurre il rischio di usi impropri della «navigazione» in *internet* (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rilevare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8, l. n. 300/1970, artt. 26 e 113 del Codice; Provv. 2 febbraio 2006, cit.). In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali: individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa; configurazione di sistemi di o utilizzo di filtri che prevengano determiniate operazioni — reputate inconferenti con l'attività lavorativa — quali l'*upload* o l'accesso a determinati siti (inseriti in una sorta di *black list*) e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato); trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni; eventuale conservazione nel tempo dei dati strettamente limitati al perseguimento di finalità organizzative, produttive e di sicurezza».

Tali oneri di organizzazione ed informativi, di tipo ovviamente preventivo, configurano una cd. *policy* interna che deve essere adeguatamente pubblicizzata e portata a conoscenza del dipendente. Tale onere di specificazione ed informazione è stato prescritto dal Garante a carico dei datori di lavoro privati e pubblici, ai sensi dell'art. 154 lett. *c*) del Codice della *privacy*.

La rilevanza dei principi sopra menzionati e degli oneri di regolamentazione ed informazione del lavoratore e dunque delle prescrizioni del Garante trova peraltro piena conferma nel fatto che l'Italia, in quanto facente parte dell'Unione europea, ha aderito ad un nucleo di valori fondamentali, previsti dall'art. 2 del Trattato di Maastricht, secondo cui «l'Unione si fonda sui valori del rispetto della

dignità umana, della libertà, della democrazia, dell'uguaglianza, della Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Strati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini». A ciò si aggiunga che la Carta dei diritti fondamentali dell'Unione europea, entrata in vigore il 1.12.2009, all'art. 7 prevede che ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni; mentre il successivo art. 8 prevede che ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano ed al trattamento di tali dati secondo il principio di lealtà, per finalità determinate ed in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge.

Ma nel caso di specie il datore non si è affatto conformato a tali principi e linee guida: nel rapporto di lavoro mancava infatti qualsiasi regola volta a disciplinare l'uso dei p.c. da parte del dipendente. In particolare proprio lo *Omissis* il più esperto nell'utilizzo dei computer e dei programmi, di fatto godeva in relazione a tali strumenti di lavoro di un'ampia libertà di movimento; egli dunque non poteva conformarsi a regole di condotta mai adottate né tantomeno aspettarsi il controllo disposto ed effettuato senza alcuna forma di preventiva informazione da cui è poi scaturito il suo licenziamento.

Pertanto alla luce di quanto previsto dall'art. 11, d.l.gs. n. 196/2003 i dati acquisiti tramite il trattamento dei dati personali non possono in alcun modo essere utilizzati ed il licenziamento che si fonda su di essi è illegittimo, e ciò a prescindere da ogni ulteriore indagine circa la effettiva riferibilità dei downloads di film e immagini erotiche al ricorrente.

Posta quindi la illegittimità del licenziamento per come sopra intimato, deve trovare applicazione il principio risarcitorio tracciato dall'art. 8, l. n. 604/1966 riconoscendo al ricorrente, in rapporto alla sua anzianità e posizione lavorativa (il rapporto intercorreva con il Centro servizi quantomeno dal 1994) e valutate tutte le circostanze del caso concreto sopra menzionate una somma corrispondente a 6 mensilità dell'ultima retribuzione globale di fatto, sulla cui entità non vi è specifica contestazione tra le parti. — *Omissis*.

IL DIFFICILE BILANCIAMENTO TRA LA TUTELA DELLA *PRIVACY* E LE ESIGENZE DI CONTROLLO DEL DATORE DI LAVORO

1. La sentenza oggetto di commento ripropone in tutta la sua problematicità la questione del difficile equilibrio che il giudice e l'ordi-

namento devono raggiungere quando la vicenda riguarda contrastanti interessi di pari valore costituzionale.

In particolare, la fattispecie verte sul caso di un lavoratore che si era rivolto al Giudice del lavoro poiché reputava che il licenziamento intimatogli fosse illegittimo per violazione degli artt. 4 e 8, St. lav., nonché delle norme del Codice della *Privacy*, d.lgs. n. 196/2003: a seguito dell'iniziativa personale del presidente dell'impresa presso cui il ricorrente era impiegato, venivano predisposti dei controlli sui computers in uso presso gli uffici della ditta (1) volti a verificare l'originalità dei programmi installati, la presenza di *password* e l'esistenza di programmi non attinenti l'attività d'impresa.

L'esito della verifica era stato particolarmente gravoso per la posizione del lavoratore poiché risultava che sul suo computer erano installati *softwares* non originali, un programma di *filesharing* per scaricare dati e film ed immagini a contenuto erotico. Inoltre vi erano anche dei documenti elettronici riguardanti attività riconducibili ad altra ditta.

Visto ciò, il datore di lavoro procedeva con il licenziamento del dipendente, ma il giudice investito della questione reputava che i dati così acquisiti non potessero essere utilizzati; pertanto considerava il recesso fondato su di essi, alla luce dell'art. 11, d.lgs. n. 196/2003, illegittimo ed anzi disponeva pure il risarcimento del danno morale subito dal lavoratore.

Sebbene il percorso giuridico seguito dall'organo giudicante per addivenire a questa conclusione appaia coerente con lo stato attuale della disciplina e sostanzialmente conforme alla giurisprudenza maggioritaria dei giudici delle leggi, forse esso non tiene del tutto conto della posizione del datore di lavoro, di alcuni orientamenti giurisprudenziali nazionali ed europei e del fatto che comunque sono stati commessi degli illeciti civili e, soprattutto, penali (2).

La verifica effettuata sul computer in uso al lavoratore è considerata dal tribunale come «trattamento dei dati personali», fattispecie prevista e disciplinata dall'art. 4 del Codice della *Privacy* che lo inquadra come «qualunque operazione o complesso di operazioni (...) concernenti la raccolta (...), la selezione (...), l'utilizzo di dati»; altresì la norma definisce dato personale: «qualunque informazione relativa a persona fisica (...), identificata (...) mediante riferimento a qualsiasi informazione».

---

(1) In realtà dalla sentenza si può solo leggere che il computer era «a lui assegnato e da lui abitualmente utilizzato», ciò mi fa credere si tratti di una postazione fissa presente in un ufficio; pertanto i rilevi che seguono attengono solo questo specifico caso. Inoltre non è dato sapere se la commissione di tali illeciti sia avvenuta durante l'orario di lavoro.

(2) Senza pretesa di completezza, si potrebbe ritenere che la normativa lesa dal lavoratore sia quantomeno quella contenuta nell'art. 171 *bis* c.p.

D'altra parte se vi è trattamento dei dati personali, è necessario seguire sia le prescrizioni dell'art. 3, Codice della *Privacy*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali in relazione alle finalità perseguite, sia l'art. 11, lett. *a* e *b*, che prevedono, rispettivamente, l'attuazione del trattamento «in modo lecito e secondo correttezza» e l'acquisizione di dati personali solo per «scopi determinati, espliciti e legittimi»; nonché la lett. *d* la quale stabilisce che essi «devono essere pertinenti (...) e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati» (3).

Inoltre, nella sua decisione, il giudice ha anche fatto riferimento alle linee guida del Garante per la protezione dei dati personali (4), che hanno chiarito, al punto 2.3 in particolare, come, assieme ad altri principi, vada osservato quello «di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori».

Da un'analisi di queste disposizioni di legge sembra emergere che il comportamento tenuto dal datore di lavoro non possa essere definito nella sua interezza *contra legem*; invero sembra di potersi affermare che non sia stato violato il principio di necessità di cui al citato art. 3.

Nel caso oggetto di commento infatti il datore di lavoro, per esigenze organizzative dell'impresa, ha svolto solo ciò che si era prefisso: la verifica degli strumenti di lavoro di sua proprietà in uso ai dipendenti (5); non risulta, quindi, esservi stato un comportamento abnorme in relazione all'uso fatto dei dati raccolti, semmai vi è stato un uso consequenziale e non astrattamente vietato.

I dati raccolti infine sono stati ottenuti proprio per conseguire «scopi determinati, espliciti e legittimi», perlomeno nelle intenzioni dell'agente: verificare se erano installati programmi vietati dalla legge all'interno dei computers in uso ai dipendenti; tra l'altro la verifica aveva comportato l'ottenimento di dati che, in relazione all'indagine espletata, sono da considerare assolutamente «pertinenti (...) e non eccedenti» rispetto alle finalità per le quali erano stati raccolti.

Non sembra rinvenirsi quindi su queste basi giuridiche l'asserito comportamento illegittimo del datore di lavoro da cui è conseguita la sanzione dell'inefficacia del recesso; semmai il solo rilievo determinante per giustificare tale conclusione, salvo quanto si dirà più oltre, potrebbe

---

(3) V. però l'art. 24, d.lgs. n. 196/2003 che esclude, in alcuni casi, la necessità del previo consenso del lavoratore.

(4) V. la deliberazione del Garante per la protezione dei dati personali, 1 marzo 2007, n. 13, G.U. 10 marzo 2007, n. 58.

(5) V. in proposito C. Zoli, *Il controllo a distanza del datore di lavoro*, *q. Riv.*, 2009, I, 496.

essere il fatto che l'acquisizione dei dati non sia avvenuta rispettando l'art. 11, lett. *a*, d.lgs. n. 196/2003, e cioè non sia avvenuta «in modo lecito e secondo correttezza». Infatti, tenendo conto anche dell'art. 4, St. lav. che è esplicitamente richiamato dall'art. 114 del Codice *Privacy*, bisogna ricordare che, al fine di contemperare al meglio il potere organizzativo del datore di lavoro con i «valori soggettivi di cui è portatore il fattore lavoro» (6), è vietato l'uso di impianti con finalità di controllo a distanza dell'attività dei lavoratori se non previamente autorizzati, onde non ledere i principi costituzionalizzati agli artt. 3, 13 e 15 Cost. di libertà personale, dignità e riservatezza.

Senonché le indicazioni legali di rango primario in tal ambito si limitano soltanto a ciò; ma poiché, come già ricordato, il giudice nelle motivazioni della sentenza richiama anche le linee guida del Garante per la protezione dei dati personali del 2007, è necessario, a questo punto, interrogarsi sul valore legale delle linee guida poiché queste dettano una specifica normativa di dettaglio che si sovrappone, anche in maniera piuttosto significativa, alla legge, tra l'altro imponendo al datore di lavoro di indicare «se, ed in che misura e con quali modalità avvengano i controlli». È corretto, in sostanza, porre sullo stesso piano le linee guida del Garante con le disposizioni della l. n. 300/1970 o del d.lgs. n. 196/2003 da un punto di vista di gerarchia delle fonti?

Non è certo questa la sede per affrontare compiutamente la questione posta, ma sembra comunque utile fissare i termini del problema tentando, inoltre, di ipotizzare una soluzione, in quanto questo provvedimento prevede obblighi e prescrizioni a carico del datore di lavoro che invece non sono previsti, perlomeno in quel modo, dalla legge (7).

Sembra di potersi affermare infatti che le deliberazioni adottate dal Garante debbono qualificarsi solo come atti amministrativi generali, cioè alla stessa stregua di una fonte regolamentare e parte della dottrina non manca di evidenziare come vi possano essere dei problemi di legittimazione (8).

Le linee guida del 2007, in base alla qualificazione giuridica da dare

---

(6) L. Mengoni, *I poteri dell'imprenditore*, *Diritto e Valori*, Il Mulino, 1985, 398.

(7) V. le considerazioni sulla tecnica di ibridazione tra discipline multilivello in materia di *privacy* di R. De Luca Tamajo, *Introduzione*, in *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, a cura di P. Tullini, *Tratt G*, LVIII, 2010.

(8) A. Rubino, *Nota alle Linee guida del Garante per la protezione dei dati personali in tema di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti* web *esclusivamente dedicati alla salute*, in *Osservatoriosullefonti.it*, 2012, I; G. De Minico, *Regole. Comando e consenso*, Giappichelli, 2004, 46, secondo cui «questo, infatti, pur non scegliendo le norme primarie da derogare, elabora in assoluta autonomia di giudizio la disciplina sostitutiva di quella primaria data l'assenza di indicazioni nella norma delegificante, il che lo colloca al di fuori della legalità costituzionale».

al *nomen* dell'istituto dovrebbero servire, semmai, ad interpretare meglio le disposizioni di legge, ad «orientare il comportamento dei destinatari» (9); in esse infatti possono rinvenirsi quelle condivisibili prescrizioni da adottare per una corretta *policy* aziendale, incentrata su un controllo cautelativo teso ad anticipare i possibili comportamenti negativi e «prevenire controlli successivi sul lavoratore». D'altra parte, rispetto a quest'ultimo punto, non si può mancare di ricordare che, in fondo nel caso di specie, il datore di lavoro si era attivato proprio per impedire il compimento — *rectius* l'aggravarsi visti i risultati — di illeciti.

In realtà il provvedimento del 2007 va ben oltre, non limitandosi ad indicare delle *best practices*, definendo piuttosto precise regole di dettaglio poste, nel caso in commento, a fondamento della decisione del giudice.

Dall'analisi del Codice della *Privacy* non sembrano emergere elementi chiarificatori della questione: infatti, sebbene l'art. 154, lett. *c* stabilisca che tra i compiti del Garante vi è quello di «prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143», quest'ultimo verte solo sulle modalità di presentazione e istruzione dei reclami da parte di chi si senta leso in un suo diritto. In conclusione, dal combinato disposto di questi due articoli si può allora ragionevolmente ritenere che «il provvedimento (del Garante) ha valore soggettivo e specifico in quanto diretto nei confronti del reclamato, non nei confronti della collettività» (10), non sembra quindi che i provvedimenti del Garante possano avere efficacia di legge e valore vincolante *erga omnes*.

2. Un ulteriore elemento, tenuto in considerazione dal giudice per dichiarare l'illegittimità del licenziamento, è poi quello relativo alle modalità con cui è stato effettuato il controllo, in quanto esso è stato giudicato del tutto occasionale e non connesso a «specifiche sospette attività illecite del dipendente»; altresì «non risultava minacciata in modo imminente la sicurezza del sistema informatico». Inoltre per lungo tempo il datore di lavoro si era totalmente disinteressato della gestione degli aspetti tecnici legati all'uso del computer dell'ufficio.

Secondo il giudicante dunque il controllo è stato illegittimo perché

---

(9) A. Rubino, *Nota alle Linee guida del Garante per la protezione dei dati personali*, cit. Ma vedi anche P. Tullini, *Comunicazione elettronica, potere di controllo e tutela*, *q. Riv*, 2009, I, 332, secondo cui l'intervento del Garante integra «i presupposti di legittimità fissati dallo Statuto con i principi cogenti in materia di trattamento dei dati».

(10) R. Zallone, *Ma il garante può legiferare? Ovvero, chi ci garantirà dal Garante?*, *www.medialaws.eu*; l'autore ricorda che «la norma affida al Garante dei compiti e non dei poteri» e che per operare come in realtà accade «dovrebbe esserci una precisa disposizione di legge che dia questo potere (non compito); ovvero ci vorrebbe una espressa delega legislativa». Dello stesso autore si segnala anche *Il Garante, i controlli, il buon senso e la legge*, *ivi*.

«improvviso, imprevisto e del tutto estemporaneo»; però se così lo si inquadra, non si tiene conto di una serie di elementi, *in primis* della recente, e non univoca per la verità, giurisprudenza in tema di controlli difensivi.

La questione infatti non è ancora stata risolta in maniera definitiva dai giudici di legittimità, tanto è vero che possono riscontrarsi sul punto due distinti orientamenti: uno che tiene fuori i controlli difensivi occulti dall'ambito di applicazione dell'art. 4, St. lav. e l'altro che, invece, reputa comunque illegittima tale attività. Quanto al primo indirizzo, una recente sentenza della Corte di Cassazione ha ribadito che, sebbene l'art. 4, St. lav. faccia parte di quella «complessa normativa diretta a contenere in vario modo le manifestazioni del potere organizzativo e direttivo del datore di lavoro che, per le modalità di attuazione incidenti nella sfera della persona, si ritengono lesive della dignità e della riservatezza del lavoratore (...) sul presupposto che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, vada mantenuta in una dimensione umana» (11), ciò nondimeno non è escluso *tout court* ogni tipo di controllo a sorpresa da parte del datore di lavoro. Quest'ultimo infatti può porre in essere attività di controllo sulle strutture informatiche aziendali che prescindono dalla sorveglianza sull'esecuzione della prestazione lavorativa e siano invece «dirette ad accertare la perpetrazione di eventuali comportamenti illeciti» (12).

Nondimeno, un'altra sentenza altrettanto recente ribadisce ulteriormente che i cd. controlli difensivi non possono tradursi in «forme surrettizie di controllo a distanza dell'attività lavorativa dei lavoratori» (13).

Nell'incertezza giudiziaria è difficile inquadrare la fattispecie oggetto

---

(11) Cass. 23 febbraio 2012, n. 2722, *GI*, I, 2013, nt. Fenucci; conforme v. Cass. 3 luglio 2001, n. 8998, *NGL*, 2002 e Cass. 3 aprile 2002, n. 4746, *GLav*, 2002, 21, 10, nt. Nogler; A. Firenze 20 ottobre 2009, *RCDL*, 2010, 1, 107, nt. Romoli che richiama ulteriore giurisprudenza.

(12) Anche parte della dottrina sembra aprire a questo tipo di ispezioni: secondo alcuni infatti i sistemi di controllo informatici sarebbero esclusi dal novero di applicazione dell'art. 4, St. lav. perché non avrebbero lo scopo primario di operare un controllo a distanza sul lavoratore: P. Ichino, *Il contratto di lavoro*, *Tratt CM*, III, 2003, 234; A. Vallebona, *Il controllo delle comunicazioni telefoniche del lavoratore*, *DL*, 2001, I, 360. V. inoltre R. De Luca Tamajo, *I controlli sui lavoratori*, in *I poteri del datore di lavoro nell'impresa*, a cura di G. Zilio Grandi, Cedam, 2002, 30; E. Gragnoli, *L'informazione nel rapporto di lavoro*, Giappichelli, 1996, 167. Per rilievi critici v. A. Bellavista, *Il controllo sui lavoratori*, Giappichelli, 1995, 65 ss.; R. Lattanzi, *Statuto dei lavoratori e protezione dei dati personali*, *q. Riv.*, 2011, I, 169 s.; F. Ravelli, *Controlli informatici e tutela della* privacy*: alla ricerca di un difficile punto di equilibrio*, *RCDL*, 2010, II, 323; P. Tullini, *Comunicazione elettronica, potere di controllo* cit., 326. V. anche la ricostruzione delle differenti posizioni dottrinarie effettuata da R. Galardi, *Il controllo sugli accessi ad* internet *al vaglio della Cassazione*, *q. Riv*, 2010, II, 564.

(13) Cass. 12 ottobre 2012, n. 17408, *D&G*, 2012, nt. Savoia; conforme Cass. 17 luglio 2007, n. 15892, *q. Riv.*, 2008, II, 718, nt. Vallauri e Cass. 23 febbraio 2010, n. 4375, *q. Riv.*, 2010, II, p. 564, nt. Galardi.

di commento in modo chiaro; se infatti si volesse seguire il primo orientamento e quindi ritenere esclusi dal campo di applicazione dell'art. 4 quei controlli difensivi aventi ad oggetto la tutela di beni estranei al rapporto di lavoro (14), la verifica della commissione, o l'interruzione della commissione, di un illecito penale non è forse una fattispecie differente dal mero e del tutto illegittimo controllo *ex post* dell'esatto adempimento della prestazione lavorativa a mezzo di strumenti elettronici (15)?

Ed infatti, se è pur vero che la possibilità di effettuare controlli difensivi si deve fermare «dinanzi al diritto alla riservatezza del dipendente, al punto che la pur insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore» (16), e se è altresì vero che i cd. controlli difensivi che riguardano l'accertamento di comportamenti dei lavoratori inerenti l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro sono assolutamente illegittimi, è però altrettanto vero che sono invece da considerarsi validi quei controlli preposti alla tutela di beni estranei al rapporto di lavoro e diretti ad accertare comportamenti illeciti dei lavoratori, come sembra essere accaduto nel caso di specie (17).

Inoltre, a corollario della vicenda, sono da aggiungere alcune considerazioni di cui bisogna pur tener conto nella difficile ricerca di un equilibrio tra le due differenti esigenze di tutela: a me sembra che è insita nella natura del «controllo» la sua estemporaneità, il suo essere occasionale, nel senso che perderebbe di molto la sua efficacia se questo non fosse effettuato in tal modo (18).

---

(14) Cass. n. 4746/2002, cit.

(15) V. anche le considerazioni di R. De Luca Tamajo, in *Introduzione*, *op. cit.*, 4 s. e P. Monda, *L'impiego dei controlli difensivi e la protezione della sfera personale del dipendente*, *DRI*, 2010, I, 192.

(16) Cass. n. 2722/2012, cit., e Cass. n. 4375/2010, cit.

(17) Cass. n. 15892/2007, cit., che dispone l'illegittimità (solamente) di tutti i controlli che riguardano l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro; Cass. 9 maggio 2007, n. 15334, *ADL*, 2007, 6, 1454, nt. Leone. V. anche T. Torino 28 settembre 2007-8 gennaio 2008, *ADL*, 2008, 2,1265, nt. Iarussi. Cfr. inoltre F. Santoni, *La* privacy *nel rapporto di lavoro: dal diritto alla riservatezza alla tutela dei dati personali*, in *Tecnologia della comunicazione e riservatezza*, *op. cit.*, 44, secondo cui «l'imposizione corretta della questione (...) consiste piuttosto nel determinare il livello di tollerabilità dell'intrusione in relazione alla natura dell'impiego e dalle specifiche circostanze». Per rilievi critici v. C. Zoli, *Il controllo a distanza del datore di lavoro*, *op. cit.*, 500 s.

(18) Si vedano anche le considerazioni di P. Ichino, *Il contratto di lavoro*, *op. cit.*, 261, secondo cui vi sarebbe il pericolo di una «cogestione generalizzata», *contra* C. Zoli, *Il controllo a distanza del datore di lavoro*, *op. cit.*, 496. V. pure A. Bellavista, *Poteri dell'imprenditore e* privacy *del lavoratore*, in *I poteri del datore di lavoro nell'impresa*, a cura di G. Zilio Grandi, *op. cit.*, 53, che reputa ragionevole il controllo difensivo di tipo «elettronico» quando sia impossibile utilizzare una forma di controllo diversa con la medesima efficacia; in questo

Infine, mi sembra che nonostante la definizione abbastanza chiara del Garante della *privacy* non tutto ciò che sia contenuto nel computer possa essere considerato «dato personale» in relazione al rapporto lavorativo; sarebbe, forse, il caso di ritenere che siano da escludere da qualsivoglia tipo di trattamento e diffusione da parte del datore di lavoro, tutti quei dati che sono connessi a posizioni strettamente personali non inerenti il rapporto di lavoro, quali le convinzioni religiose, le opinioni politiche o i dati medici ed in generale tutti quegli elementi tali da presupporre una discriminazione ai danni del lavoratore così come previsto dall'art. 8, St. lav (19). Tutt'altra fattispecie, e quindi altra valutazione potrebbe essere fatta invece in relazione a quei dati che, seppur personali, sono addirittura frutto della commissione di un reato penale o comunque sono stati acquisisti al di fuori dei canoni di diligenza, correttezza e buona fede nell'esecuzione della prestazione previsti dagli artt. 2104, 1175 e 1375 c.c. (20).

3. La condanna del datore di lavoro è avvenuta anche perché si è ritenuto leso l'art. 2 del Trattato di Maastricht secondo cui tra i molti diritti su cui si fonda l'Unione europea vi è quello della dignità umana, altresì violati sarebbero stati gli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea che prevedono, rispettivamente, il diritto di ogni individuo al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni, ed il diritto alla protezione dei dati di carattere personale ed al loro trattamento secondo il principio di lealtà (21).

Senonché, non si può nascondere che quest'ultimo principio non è riferibile ad una soltanto delle parti, ma spiega, semmai, i suoi effetti sull'intero rapporto; inoltre la medesima normativa europea apre ad una compressione dei diritti delle parti quando se ne ravvisi la necessità: l'art. 8 della Carta, infatti, prevede che il trattamento dei dati personali possa

---

senso anche N. Ghirardi, *Ancora in materia di controlli occulti sui dipendenti*, *q. Riv.*, 2007, II, 888.

(19) V. le considerazioni sulle tutele antidiscriminatorie di F. Santoni, *La* privacy *nel rapporto di lavoro: dal diritto alla riservatezza alla tutela dei dati personali*, *op. cit.*, 28.

(20) M. Persiani, *Sul controllo dei poteri del datore*, *DL*, 1995, 139, secondo cui «nell'esecuzione del contratto ciascuno dei contraenti è tenuto a salvaguardare l'interesse dell'altro anche al di là della disciplina legale»; E. Gragnoli, *Dalla tutela della libertà alla tutela della dignità e della riservatezza dei lavoratori*, *ADL*, 4, 2007, 1228 s., secondo cui «il punto debole è il concetto di «dato», scisso dal processo psichico di cui è il risultato». V. anche Cass. n. 8998/2001, cit., in cui, addirittura, si sostiene che il controllo può avvenire «indipendentemente dalle modalità» ed «anche occultamente».

(21) V. le considerazioni di A. Sitza, *Il problema dell'accesso alla posta elettronica aziendale da parte del datore di lavoro tra segretezza della corrispondenza e limiti del potere di controllo*, *NGCC*, 2008, 960 s.

avvenire per determinate finalità basate su «altro fondamento legittimo previsto dalla legge» e forse, in tal senso potrebbe essere inteso il controllo teso ad evitare la commissione di un reato penale.

Del resto, la Corte europea dei diritti dell'uomo non è nuova a forme di contemperamento dei contrapposti interessi in gioco e sembra seguire questa direzione quando ricorda come nella valutazione complessiva della fattispecie bisogna determinare se sia stato raggiunto «un giusto equilibrio tra gli interessi in gioco: 1. la vita privata (*privacy*); 2. l'interesse del datore di lavoro a difendere la sua proprietà; 3. l'interesse pubblico alla corretta amministrazione della giustizia» (22); non vi è quindi preminenza di un diritto su un altro, ma normale contemperamento degli interessi. Tale orientamento sembra essere anche quello seguito dalla sezione lavoro della Corte di Cassazione, la quale ha ritenuto non esservi nel nostro ordinamento un assoluto e generale diritto alla *privacy*, piuttosto reputa che, nei casi di contrapposizione di diritti garantiti dalla Costituzione, debba adottarsi la cd. gerarchia mobile: «principio da intendersi non come rigida e fissa subordinazione di uno degli interessi all'altro, ma come concreta individuazione da parte del giudice dell'interesse da privilegiare tra quelli antagonistici a seguito di una ponderata valutazione della specifica situazione sostanziale dedotta in giudizio con conseguente bilanciamento tra gli stessi, capace di evitare che la piena tutela di un interesse possa tradursi nella limitazione di quello contrapposto tanto da vanificarne o ridurne il valore contenutistico» (23). Di simile tenore anche una precedente sentenza del 2009, la quale aggiunge che «in tema di trattamento dei dati personali, l'interesse alla riservatezza, tutelato dall'ordinamento positivo, recede quando quest'ultimo sia esercitato per la difesa di un interesse giuridicamente rilevante e nei soli ovvi limiti in cui esso sia necessario alla tutela» (24).

4. Infine un ulteriore aspetto, spesso dimenticato, da tenere in considerazione in questa difficile ricerca di un equilibrio, è poi quello relativo al valore da dare all'elemento della fiducia e al suo immediato corrispettivo, cioè la fedeltà nello svolgimento del rapporto lavorativo. È bene ricordare infatti che la fiducia è uno dei valori che connette uno specifico lavoratore con l'organizzazione dell'impresa ed è un'estrinseca-

---

(22) In Cedu 5 ottobre 2010, n. 420, *Kopke* c. *Germania*, *CP*, V, 2011, 1972 la Corte ha ritenuto legittimo sottoporre a videosorveglianza occulta una lavoratrice con l'ausilio di una società di investigazione. In senso contrario Cedu 3 aprile 2007, n. 62617, *Copland* c. *Regno Unito*, *GDA*, 2007, VI, 644.

(23) Cass. 5 agosto 2010, n. 18279, *RCDL*, 2010, 4, 1143, nt. Cafiero.

(24) Cass. 30 giugno 2009, n. 15327, *RCDL*, 2009, 3, 695, nt. Bonsignorio.

zione del potere organizzativo del datore di lavoro (25). D'altronde, nonostante un certo processo di spersonalizzazione del rapporto lavorativo portato avanti da parte della dottrina (26), la sua mancanza è un elemento che, secondo la giurisprudenza della Suprema corte, può ben giustificare l'interruzione del rapporto (27), in quanto il lavoratore deve astenersi dal tenere tutti quei comportamenti che, oltre ad apparire «in contrasto con i doveri connessi all'inserimento del lavoratore nella struttura e nell'organizzazione dell'impresa (...) sono idonei comunque a ledere irrimediabilmente il presupposto fiduciario del rapporto stesso» (28).

Del pari non può omettersi di valutare che, nel caso oggetto di commento, i controlli erano pur stati predisposti per prevenire o addirittura interrompere la commissione di un reato di natura penale. Orbene la *ratio*, e la finalità stessa della legge sulla *privacy*, non è certo quella di proteggere il lavoratore dall'accertamento della commissione degli illeciti siano essi pensali o civili (29). Da questo punto di vista, per come si realizza attualmente il contemperamento degli interessi in gioco, non sembra si sia raggiunto un punto di equilibrio ragionevole (30).

Filippo Olivelli
Ricercatore di diritto del lavoro nell'Università di Macerata

---

(25) M. Persiani, *Contratto di lavoro e organizzazione*, Cedam, 1966; P. Tosi, Intuitus personae *e fiducia*, *ADL*, 2012, 3, 541.

(26) V. la ricostruzione di C. Pisani, *Licenziamento e fiducia*, Giuffrè, 2004.

(27) La Corte di Cassazione reputa legittimo punire con il licenziamento il comportamento del lavoratore che si disinteressa colpevolmente delle esigenze del datore di lavoro reiterando più volte la condotta lesiva, v. Cass. n. 15334/2007, cit., e Cass. 10 luglio 2002, n. 10062, *MGL*, 2002, 644, nt. Bertocchi; Cass. 19 dicembre 2000, n. 15919, *DPL*, 2001, 1524. Altresì v. le considerazioni di G. Leone, *Un caso di licenziamento per giusta causa per indebito utilizzo personale del telefono cellulare*, *op. cit.*, 1459, e S. Caffio, *Poteri datoriali e tutela della riservatezza del lavoratore: note a margine di una sentenza di merito*, *q. Riv.*, 2008, II, 840 secondo cui (in ambito bancario) «l'affidabilità imposta dalla delicatezza delle mansioni attribuite al ricorrente sarebbe tale — secondo l'impostazione seguita nella sentenza commentata — da estendersi alla vita extralavorativa del soggetto».

(28) Cass. 10 dicembre 2008, n. 29008, *q. Riv.*, 2009, II, 918, nt. Santini; v., più in generale, le considerazioni P. Tosi, Intuitus personae *e fiducia*, *op. cit.*, segnatamente 544 e 546, secondo cui «della rilevanza della fiducia e del suo corrispettivo fedeltà non è possibile affrancarsi (...) se non al prezzo dello scollegamento dal diritto vivente».

(29) In questo senso v. T. Torino 8 gennaio 2008, *q. Riv.*, 2008, II, 854 in cui può leggersi «la *privacy* è infatti bene troppo prezioso (...) per immaginare che la sua garanzia possa innestarsi su condotte che contravvengono ai doveri professionali ed essere quindi terreno per coprire attività abusive e mezzo per evitare strumentalmente di doverne rispondere».

(30) V. anche le considerazioni di P. Tullini, *Tecnologie informatiche in azienda: dalle linee—guida del garante alle applicazioni concrete*, in *Tecnologie della comunicazione* cit., 133, secondo cui il Garante sacrifica l'esigenza di responsabilizzazione di chi commette l'illecito.