18302/16

REPUBBLICA ITALIANA

IN NOME DEL POPOLO ITALIANO

LA CORTE SUPREMA DI CASSAZIONE

PRIMA SEZIONE CIVILE

Oggetto: Privacy - Rapporto di lavoro - Internet, Posta elettronica, telefonia - Controlli difensivi - Limiti - Violazione degli artt. 4 ed 8 della legge n. 300 del 1970

Composta dagli Ill.mi Signori Magistrati

Dott. RENATO BERNABAI Presidente

Dott. MARIA CRISTINA GIANCOLA Consigliere

Dott. GIACINTO BISOGNI Consigliere

Dott. CARLO DE CHIARA Consigliere

Dott. ANTONIO PIETRO LAMORGESE Consigliere rel.

R.G.N. 22145/2013

Cron. 18302 Rep. C.I.

Ud. 24/06/2016

Ha pronunciato la seguente

SENTENZA

sul ricorso n. 22145-2013 proposto dall'Istituto Poligrafico e Zecca dello Stato S.p.a., in persona del legale rappresentante *pro-tempore*, rappresentato e difeso, in virtù di mandato in calce al ricorso introduttivo, dagli Avvocati Paolo Ricchiuto e Francesca Colavincenzo, ed elettivamente domiciliato in Roma alla via Oslavia n. 30, presso lo studio degli Avvocati Giovanni Guerra e Paolo Ricchiuto;

- ricorrente -

contro

Garante per la protezione dei dati personali, in persona del legale rappresentante *pro tempore*, rappresentato e difeso dall'Avvocatura Generale dello Stato, presso cui elettivamente domicilia in Roma alla via dei Portoghesi n. 12;

- controricorrente -

avverso

la sentenza n. 1196/2013 della prima sezione civile del Tribunale di Roma, depositata il 4 aprile 2013.

Dato atto che parte ricorrente ha depositato memoria ai sensi dell'art. 378 C.p.c.;

sentita la relazione della causa svolta nella pubblica udienza del giorno 24 giugno 2016 dal relatore dott. Antonio Pietro Lamorgese;

udito, per il ricorrente, l'Avv. P. RICCHIUTO che ha chiesto la remissione atti alle SS.UU.;
udito, per il controricorrente, l'Avvocato Gen. dello Stato W. FERRANTE che ha chiesto il rigetto del ricorso;
udito il P.M. in persona del sostituto procuratore generale Dott. Lucio Capasso, che ha concluso per il rigetto del ricorso.

RITENUTO IN FATTO

L'Istituto Poligrafico e Zecca dello Stato spa impugnava, innanzi al Tribunale di Roma, il provvedimento, emesso dal Garante per la Protezione dei Dati Personali il 21 luglio 2011, con il quale era stato vietato al Poligrafico l'ulteriore trattamento, nelle forme della conservazione e della categorizzazione, dei dati personali dei dipendenti, relativi: alla navigazione *Internet*, all'utilizzo della posta elettronica ed alle utenze telefoniche chiamate dai lavoratori, con contestuale imposizione dell'obbligo di informare gli utenti del trattamento dei dati personali.
Il Garante aveva richiesto l'adozione di misure idonee ad assicurare che fosse resa nota ai dipendenti l'identità degli amministratori di sistema abilitati ad accedere alle banche dati aziendali e che fosse assicurata la completezza del tracciamento di tutti gli accessi effettuati da detti amministratori.
Infatti aveva evidenziato, nel provvedimento sanzionatorio, che il servizio di navigazione in *Internet* predisposto dal ricorrente per i propri dipendenti non si limitava a rifiutare la connessione dei lavoratori ai siti *Web* non inerenti l'attività del Poligrafico, ma memorizzava ogni accesso, ed anche ogni tentativo di accesso, generando la possibilità di ricostruire la navigazione di ogni singolo lavoratore, conservandosi i dati nel sistema per una durata variabile da sei mesi ad un anno. Di conseguenza, il Garante aveva ritenuto integrata la violazione degli

articoli 4 ed 8 della legge n. 300 del 1970 (Statuto dei Lavoratori), per la possibilità di rilevare dati sensibili dei lavoratori senza aver acquisito il previsto consenso degli interessati, conseguendo da tale condotta anche la violazione degli artt. 11, 113 e 114 del Codice sulla protezione dei dati personali.

Altrettanto censurabile era il sistema di conservazione sul *server* aziendale dei messaggi di posta elettronica inviati e ricevuti dai dipendenti, che ne prevedeva la conservazione per prolungato periodo di tempo e ne consentiva la visualizzazione integrale da parte degli amministratori di sistema, senza che fosse stata fornita alcuna specifica informativa in merito. Censurabile risultavano anche le modalità di controllo del traffico telefonico attuato dal Poligrafico mediante il sistema *VoIP*, che consentiva la registrazione e la prolungata conservazione dei dati del traffico, anche in questo caso senza che fosse stata fornita un'adeguata informazione all'utenza; inoltre, il sistema di captazione dei dati comportava l'acquisizione di *frame* presenti sulle pagine visualizzate ma non riconducibili a scelte dell'utente (pubblicità, *pop-up*, etc.).

Il Tribunale di Roma, con provvedimento del 4 aprile 2013, ricordava che l'art. 4, primo comma, dello Statuto dei Lavoratori vieta al datore di lavoro l'uso di impianti audiovisivi o altre apparecchiature con finalità di controllo a distanza dell'attività dei lavoratori. Il medesimo articolo, al secondo comma, chiarisce che gli impianti e le apparecchiature di controllo "che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro" - da includersi nei cd. "controlli difensivi" in senso ampio - "ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere istallati

soltanto previo accordo con le rappresentanze sindacali [e] in difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro".

Pertanto, l'utilizzazione di tali impianti ed apparecchiature per esigenze organizzative e produttive è consentita al datore di lavoro ma solo a condizione di raggiungere un'intesa con le rappresentanze sindacali dei lavoratori oppure a seguito dell'espletamento delle procedure suppletive indicate dalla legge; mentre la loro utilizzazione è senz'altro vietata se attuata con la specifica finalità di esercitare una vigilanza sull'attività dei lavoratori.

Il Tribunale di Roma ha ricostruito l'evoluzione della giurisprudenza di legittimità in materia, evidenziando che, a seguito di una prima pronuncia che aveva ritenuto i cd. controlli difensivi estranei all'ambito applicativo dell'art. 4 dello Statuto dei lavoratori, pronunce successive avevano condivisibilmente osservato che il rispetto delle esigenze di tutela aziendale non poteva condurre a ritenere legittima la soppressione di diritti fondamentali del dipendente, come la riservatezza, e che la ricordata disposizione della legge n. 300 del 1970 trova applicazione anche in materia di cd. controlli difensivi, tutte le volte che le modalità di esecuzione dei controlli previste dal datore di lavoro comportino anche la possibilità di un controllo a distanza dei lavoratori.

Di conseguenza, il Tribunale ha rigettato il ricorso dell'Istituto Poligrafico.

Avverso la decisione del Tribunale di Roma l'Istituto Poligrafico ha proposto ricorso per cassazione, affidato a cinque motivi. Ha resistito con controricorso il Garante per la Protezione dei Dati Personali.

CONSIDERATO IN DIRITTO

Preliminarmente deve ricordarsi che il ricorrente ha domandato rimettersi la decisione del ricorso alle Sezioni Unite della Corte, in quanto occorre decidere su una questione di diritto già decisa in senso difforme dalla giurisprudenza di legittimità e perché trattasi di questione di massima di particolare importanza. Non si ritiene, però, di accogliere questa sollecitazione, perché la giurisprudenza di legittimità, dopo una pronuncia diretta in senso parzialmente contrario, ha poi adottato una linea interpretativa evolutiva e coerente, cui il Collegio ritiene di dare continuità.

1. Con il primo motivo di impugnazione (in cui possono esaminarsi congiuntamente i motivi indicati come I, Ia, Ib e II), l'Istituto Poligrafico e Zecca dello Stato ha dedotto, ai sensi dell'art. 360, n. 3, c.p.c., la violazione e falsa applicazione degli artt. 4 e 8, della legge n. 300 del 1970 (Statuto dei lavoratori), e degli artt. 12 e 14 disp. prel. c.c., nonché 11, primo comma, lett. a), c) e d), e 113 e 114 Codice Privacy (D.Lgs. n. 196 del 2003), per avere il Tribunale di Roma ritenuto applicabile alla fattispecie l'art. 4 cit., secondo comma, e non operativa la categoria dei controlli difensivi.
Secondo il ricorrente, l'art. 4 "non esaurisce tutte le ipotesi di controllo del datore di lavoro sulla condotta tenuta dal lavoratore in azienda intesa nella sua ampiezza, per la semplicissima ragione che quella norma regolamenta solo il profilo attinente il controllo sull'attività lavorativa ... rimangono completamente fuori dal confine operativo della norma i controlli che abbiano ad oggetto non l'attività lavorativa, ma altri comportamenti tenuti dal lavoratore sul posto di lavoro, e segnatamente quelli illeciti, che espongano ad un pericolo i beni dell'azienda e/o concretino fatti potenzialmente dannosi per i terzi,

con conseguente responsabilità del datore di lavoro". Trattasi di esigenza che assumerebbe in questo caso un particolare rilievo, in considerazione delle attribuzioni di interesse pubblicistico assegnate all'Istituto Poligrafico, come la stampa della Gazzetta Ufficiale e della Raccolta ufficiale degli atti normativi della Repubblica italiana, la produzione di documenti identificativi della persona, di sistemi di sicurezza e anticontraffazione, di monete, ecc. Nella prospettazione del ricorrente, "il tratto distintivo dell'art. 4, tanto al primo quanto al secondo comma, è ravvisabile nell'aver circoscritto il proprio campo di applicazione solo ed esclusivamente al controllo 'sull'attività lavorativa dei dipendenti'". Nel caso di specie, i controlli predisposti dal Poligrafico non atterrebbero alle esigenze organizzative e produttive ovvero alla sicurezza del lavoro, di cui all'art. 4, secondo comma, dello Statuto dei lavoratori, bensì ad esigenze di "tutela del patrimonio aziendale".

Con riferimento alla navigazione in *Internet* da parte dei dipendenti, l'utilizzazione del sistema *Websense* era stata prevista proprio per la finalità di rispettare le esigenze di prevenzione volte a ridurre il rischio di utilizzazioni improprie della navigazione, ed è per questo che il sistema assicurava che determinati siti fossero inaccessibili dalla rete aziendale. Il Tribunale erroneamente aveva condiviso le censure del Garante, in materia di conservazione dei dati relativi alla navigazione in *Internet* di ciascun dipendente, mentre i dati venivano conservati per finalità di tutela aziendale e per potere, se del caso, informare l'Autorità Giudiziaria di eventuali illeciti. Inoltre, la navigazione in *Internet*, se non controllata, comporterebbe la possibilità di rischi (come la possibilità di acquisire virus nella rete aziendale) che un'azienda con le

attribuzioni pubblicistiche proprie del Poligrafico non può consentire.

In ogni caso, l'art. 8 dello Statuto dei lavoratori vieta la "effettuazione" attiva delle indagini sulle opinioni politiche, religiose o sindacali dei dipendenti e non già la mera possibilità di effettuazione delle medesime.

Quanto alla presunta violazione dell'art. 11 del Codice Privacy e del principio di pertinenza e non eccedenza dei controlli, se non vi fosse la possibilità di acquisire e conservare i dati identificativi dei contatti *Internet* (utente che richiede il contatto, sito contattato o che si tenta di contattare, data ed ora dell'accesso o del tentativo), sarebbe preclusa la tutela delle ragioni di sicurezza, sicché anche questa materia dovrebbe essere ricondotta nell'alveo dei cd. controlli difensivi.

1.1 Il motivo è infondato.

E' opportuno premettere che il rilievo pubblicistico dei compiti affidati all'Istituto Poligrafico dello Stato non è idoneo a giustificare la violazione della normativa vigente, che intende assicurare garanzia ai diritti costituzionalmente riconosciuti ai lavoratori, in primo luogo al diritto alla riservatezza.

Il ricorrente afferma, in sostanza, che spetta al datore di lavoro predisporre tutti gli strumenti necessari per la tutela dei beni aziendali rispetto a possibili danni ed accertare e prevenire comportamenti illeciti dei dipendenti, purché non abbiano quale scopo diretto la vigilanza sulla prestazione di lavoro fornita dai dipendenti (art. 4, primo comma, legge n. 300 del 1970) e non siano finalizzati alla tutela di esigenze organizzative e produttive, ovvero della sicurezza del lavoro (art. 4, secondo comma, legge cit.).

E' necessario esaminare l'art. 4 dello Statuto dei Lavoratori.

Esso prevede, al primo comma, il divieto assoluto per il datore di lavoro di utilizzare "impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori", ma non è questa la contestazione rivolta all'Istituto Poligrafico, non risultando che i controlli sulla navigazione in Internet e sull'utilizzo dei servizi di telefonia e posta elettronica siano stati specificamente predisposti per finalità di vigilanza a distanza dell'attività lavorativa dei dipendenti.

Il secondo comma prevede che "gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere istallati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti". Nel giudizio in esame è pacifico che il ricorrente Istituto Poligrafico non ha mai ricercato un accordo con le rappresentanze dei lavoratori al fine di disciplinare i controlli, e neppure ha promosso le procedure suppletive che la legge prevede siano svolte qualora un accordo non sia raggiunto.

Si deve operare, in materia, un contemperamento tra i diritti del datore di lavoro e, in particolare, alla libera iniziativa economica ed alla protezione dei beni aziendali, con la tutela dei diritto del lavoratore, in primo luogo alla riservatezza. Questo bilanciamento non è affidato alla valutazione della giurisprudenza, avendo il legislatore

provveduto a dettare la disciplina generale della materia, in primo luogo proprio mediante le norme previste dall'art. 4 dello Statuto dei lavoratori. Per comprenderne l'esatta portata, è necessario esaminare, oltre il suo testo letterale, anche la finalità della norma.

La disposizione di cui all'art. 4, secondo comma, in esame - collocata nel Titolo I dello Statuto, che prescrive regole per la tutela della libertà e dignità del lavoratore - è rivolta ad assicurare al lavoratore che il controllo a distanza, anche solo potenziale, della sua attività lavorativa sia protetto da garanzie, qualunque sia la finalità per la quale il datore di lavoro predispone i controlli. Quando l'attività di vigilanza a distanza, attivata dal datore di lavoro per qualsiasi finalità, permetta anche la mera "possibilità di controllo dell'attività lavorativa" fornita dal prestatore di lavoro, l'attività non è consentita se non a seguito del positivo esperimento delle procedure di garanzia di cui all'art. 4, secondo comma, del medesimo Statuto. Non è possibile ritenere che il datore di lavoro possa liberamente utilizzare impianti e apparecchiature di controllo per qualsiasi finalità (di tutela dei beni aziendali, di accertamento e prevenzione dei comportamenti illeciti dei dipendenti, ecc.), eludendo il positivo esperimento delle procedure previste nel secondo comma dell'art. 4 in esame, quando derivi anche solo "la possibilità di controllo a distanza dell'attività dei lavoratori", a prescindere dalle sue intenzioni.

Questa conclusione non si pone in contrasto con l'evoluzione della giurisprudenza di legittimità in materia.

E' vero che una risalente decisione della Suprema Corte aveva affermato che il controllo diretto ad accertare condotte illecite del lavoratore, cd. controllo difensivo,

non sarebbe assoggettato alla disciplina di cui all'art. 4 dello Statuto dei lavoratori (Cass., Sez. L., n. 4746 del 2002). Questo orientamento ha ricevuto però smentita da una successiva pronuncia di questa Corte, la quale ha precisato che "la garanzia procedurale prevista per impianti ed apparecchiature ricollegabili ad esigenze produttive contempera l'esigenza di tutela del diritto dei lavoratori a non essere controllati a distanza e quello del datore di lavoro o, se si vuole, della stessa collettività, relativamente alla organizzazione, produzione e sicurezza del lavoro, individuando una precisa procedura esecutiva e gli stessi soggetti ad essa partecipi"; ha quindi chiarito che l'utilizzo di un'apparecchiatura comunque idonea ad esercitare la vigilanza a distanza sui prestatori di lavoro, si risolve "in un controllo … rientrante nella fattispecie prevista dal secondo comma dell'art. 4 della legge n. 300 del 1970, né l'esigenza di evitare condotte illecite da parte dei dipendenti può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore" (Cass. Sez. L., n. 15892 del 2007).

La suddetta linea interpretativa, contrariamente a quanto affermato dal ricorrente, ha ricevuto molteplici conferme nella giurisprudenza di questa Corte. Ad esempio, in un caso in cui il datore di lavoro utilizzava programmi informatici che consentivano il monitoraggio della posta elettronica e degli accessi *Internet* dei dipendenti, il Giudice di legittimità ha ritenuto applicabili le "garanzie procedurali imposte dall'art. 4, secondo comma, della legge n. 300 del 1970… per l'istallazione di impianti ed apparecchiature di controllo… dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori", dopo avere evidenziato la necessità di contemperare le esigenze del datore di lavoro con i diritti

del prestatore di lavoro; pertanto, anche i controlli cd. difensivi "diretti ad accertare comportamenti illeciti dei lavoratori", quando comportino la possibilità del controllo a distanza della prestazione lavorativa dei dipendenti, sono soggetti alla disciplina di cui all'art. 4, secondo comma, dello Statuto dei lavoratori (v. Cass., Sez. L., n. 4375 del 2010, n. 16622 del 2012, le quali affermano che "la possibilità di effettuare tali controlli incontra un limite nel diritto alla riservatezza del dipendente, tanto che anche l'esigenza di evitare condotte illecite dei dipendenti non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore").

Di recente, questa Corte ha confermato che un'apparecchiatura predisposta dal datore di lavoro ("badge" idoneo a controllare l'ingresso e l'uscita del dipendente, ma anche le pause ed i permessi, ed a comparare nell'immediatezza i dati di tutti i dipendenti) "ove sia utilizzabile anche in funzione di controllo a distanza del rispetto dell'orario di lavoro e della correttezza dell'esecuzione della prestazione … è illegittima, ai sensi dell'art. 4, comma 2, della l. n. 300 del 1970, se non concordata con le rappresentanze sindacali, ovvero autorizzata dall'Ispettorato del lavoro, dovendosi escludere che l'esigenza di evitare condotte illecite da parte dei dipendenti possa assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore" (Cass., Sez. L., n. 9904 del 2016).

Corretta è anche la contestazione del Garante, confermata dal Tribunale, relativa alla violazione del disposto di cui all'art. 8 dello Statuto dei lavoratori. La norma prevede che è vietato al datore di lavoro "effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose

o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore". Ed acquisire e conservare dati che contengono (o possono contenere) simili informazioni importa già l'integrazione della condotta vietata, perché si risolve in una indagine non consentita sulle opinioni e condotte del lavoratore, anche se i dati non sono successivamente utilizzati. Non è necessario sottoporre i dati raccolti ad alcun particolare trattamento per incorrere nell'illecito, poiché la mera acquisizione e conservazione della disponibilità di essi comporta la violazione della prescrizione legislativa.
Il motivo deve essere, pertanto, disatteso.

2. Con il secondo motivo (nn. IIa, IIb), l'Istituto ricorrente ha denunciato, ai sensi dell'art. 360, n. 3, c.p.c., la violazione o falsa applicazione dell'art. 4 dello Statuto dei lavoratori e degli artt. 12 e 14 disp. prel., perché la natura di controllo difensivo dell'attività posta in essere escluderebbe l'applicabilità della normativa indicata. Inoltre, è contestato, ai sensi dell'art. 360, n. 5, c.p.c., l'omesso esame di un fatto decisivo per il giudizio, costituente oggetto di discussione tra le parti, per non avere il Tribunale pronunciato sulle modalità di utilizzo dei dati raccolti mediate il *software Websense* con finalità esclusiva di controllo difensivo.
Il ricorrente ha confermato di avere inibito ai dipendenti l'accesso a determinati siti *Internet* considerati pericolosi e provveduto alla registrazione dei cd. *file Log* (identificativi di indirizzo *Ip*, cioè della postazione di lavoro, dell'utenza contattata, della data ed ora dell'accesso o del tentativo di accesso), ma ha affermato che si tratta di un'attività svolta per esclusiva finalità

di tutela aziendale. Si dovrebbe tenere conto che i lavoratori erano stati resi edotti del fatto che i file di log venivano registrati con questa finalità, che la mancata registrazione precluderebbe la prevenzione ed esporrebbe l'Istituto ad attacchi non identificabili alla rete aziendale. In ogni caso, non sarebbe configurabile alcuna violazione dell'art. 8 dello Statuto dei lavoratori, che vieta la "effettuazione" attiva delle indagini sulle opinioni politiche, religiose o sindacali dei dipendenti, e non la mera possibilità di effettuazione delle medesime, non avendo l'Istituto mai effettuato alcuna indagine sui profili extraprofessionali dei lavoratori.

2.1 Il motivo è inammissibile nella parte in cui denuncia, da un lato, una insufficienza motivazionale che non è più censurabile, a norma del novellato art. 360 n. 5 c.p.c. (v. Cass., Sez. Un., n. 8053 del 2014) e, dall'altro, la prevalenza attribuita dal Giudice di merito, nel percorso motivazionale, ad alcune circostanze piuttosto che ad altre, implicitamente respinte, le quali sono prive del carattere della decisività, nel senso che una diversa valutazione delle stesse non avrebbe determinato un esito diverso della decisione.

Infatti, si è già argomentato in ordine all'obbligo di portare positivamente a compimento le procedure di cui all'art. 4, secondo comma, dello Statuto dei lavoratori, quando l'attività di vigilanza sia anche solo potenzialmente idonea a comportare il controllo dell'attività svolta dai lavoratori.

Nel giudizio di merito si è accertato che il Poligrafico provvedeva - non solo alla, di per sé lecita, inibizione dell'accesso dei lavoratori a determinate categorie di siti *Internet*, ma anche - alla registrazione dei cd. *file Log* (identificativi di indirizzo *Ip*, cioè della postazione di

lavoro, dell'utenza contattata, della data ed ora dell'accesso o del tentativo di accesso), senza che fossero state espletate le procedure previste dalla legge per lo svolgimento delle attività che comportino anche solo la possibilità di controllo a distanza dei lavoratori. Ed è irrilevante che i lavoratori fossero stati messi a conoscenza delle modalità di acquisizione dei dati di traffico, conservati per un periodo di tempo prolungato (da sei mesi a un anno).

Inoltre, la acquisizione e conservazione dei dati relativi alla navigazione Internet dei dipendenti mediante captazione e registrazione dei file Log importa la violazione anche del disposto di cui all'art. 8 della legge n. 300 del 1970, per le ragioni innanzi indicate (v., *supra*, 1.1, in fine).

Il motivo è rigettato.

3. Con il terzo motivo di ricorso (nn. IIIa, IIIb), in riferimento alla gestione del servizio di posta elettronica, il Poligrafico ha contestato, ai sensi dell'art. 360, n. 3, c.p.c., la violazione o falsa applicazione degli artt. 2 e 13 del Codice della Privacy, per avere il Tribunale censurato la condotta del Poligrafico per non avere fornito ai lavoratori una informazione adeguata sulle modalità di trattamento dei dati, in relazione alla conservazione di quelli relativi alle comunicazioni in chiaro, e limitatamente ai lavoratori che avessero deciso di avvalersi del *server* aziendale per la conservazione dei messaggi di posta elettronica. Si assume che tale informazione non fosse prevista dalle citate norme, ma eventualmente dalle Linee Guida sulla Posta Elettronica ed Internet, emanate dal Garante il 1°.3.2007, disciplina la cui violazione (cfr. art. 154, comma 1, lett. c, del Codice della Privacy) non era stata

contestata al ricorrente. Inoltre, sempre con riferimento al servizio di posta elettronica, è denunciato, ai sensi dell'art. 360, comma 5, c.p.c., l'omesso esame circa un fatto decisivo per il giudizio, costituente oggetto di discussione tra le parti, per non avere il Tribunale pronunciato in ordine alla completezza dell'informazione assicurata dal Poligrafico ai propri dipendenti. E' stato evidenziato che ad ogni singolo utente era lasciata la facoltà di far conservare i messaggi *e-mail* sulla *mailbox* aziendale e che ciò attestava come i dipendenti fossero ben informati e consapevoli del fatto che la scelta effettuata comportava che i messaggi rimanevano conservati anche sul server ed erano accessibili agli amministratori del sistema; che era attivo un servizio di *help-desk* per la configurazione del servizio di posta elettronica, a disposizione dei lavoratori, i quali potevano ricevere idonee informazioni circa le possibili modalità di configurazione del servizio; che dal documento PR-FSIA2-209, che si afferma essere stato distribuito al personale, erano ricavabili "indicazioni" che consentivano di apprendere che la Unità Organizzativa Gestione Sistemi dell'Area ICT e *Business Solutions* avrebbe potuto accedere alle risorse informatiche dell'utente, ai fini di sicurezza del sistema; infine, sulla rete *intranet* aziendale, consultabile da qualsiasi dipendente, sin dal marzo 2010, erano indicati gli identificativi degli amministratori di sistema abilitati ad accedere ai dati raccolti nel sistema informatico del Poligrafico.

3.1 Il Giudice di merito ha reso una motivazione, pienamente adesiva alle argomentazioni del Garante, adeguata e non censurabile sotto il profilo della insufficienza (a norma del nuovo art. 360 n. 5 c.p.c.), in ordine alla illiceità del trattamento relativo ai servizi

di posta elettronica. Il ricorrente deduce, in questa sede, varie circostanze di fatto - ritenute implicitamente irrilevanti dal Giudice di merito - e chiede impropriamente al Giudice di legittimità di esaminarle, senza neppure spiegare se e in quale atto siano state fatte valere nel giudizio di merito.

Si obietta che a tutti i lavoratori erano state fornite informazioni specifiche, idonee a soddisfare le prescrizioni di cui all'art. 13 del Codice della Privacy, mediante la consegna di documenti non prodotti, però, nella fase ispettiva e il cui contenuto non è stato trascritto nel ricorso.

Inoltre, il fatto di aver fornito informazioni ai propri dipendenti non è elemento decisivo per escludere la violazione del disposto di cui all'art. 4, secondo comma, dello Statuto dei lavoratori.

Deve aggiungersi che quand'anche si informino i lavoratori della possibilità di archiviare i messaggi di posta elettronica sul *server* aziendale oppure sul PC messo a disposizione dall'azienda, questo non comporta che essi siano resi edotti che, scegliendo la prima opzione, i loro messaggi rimarranno, per un periodo di tempo prolungato, accessibili in chiaro dai soggetti abilitati alla consultazione.

Il motivo è rigettato.

4. Con il quarto motivo (nn. IVa e IVb), il ricorrente ha contestato, ai sensi dell'art. 360, numero 3, c.p.c., la violazione e falsa applicazione dell'art. 4 dello Statuto dei lavoratori e degli artt. 12 e 14 disp. prel. c.c. nonché, ai sensi dell'art. 360, n. 5, c.p.c., l'omesso esame circa un fatto decisivo per il giudizio, costituente oggetto di discussione tra le parti, in relazione all'esercizio del servizio di telefonia.

Si assume che il Tribunale abbia omesso di pronunciare sulle argomentazioni dell'Istituto Poligrafico, di seguito riportate.

Il servizio di telefonia, cd. sistema *VoIP*, veniva gestito mediante l'applicativo *Blue's*, grazie al quale il Poligrafico aveva accesso ai dati raccolti e conservati dal sistema, configurato in modo da rilevare eventuali telefonate ingiustificate effettuate dalle utenze assegnate ai dipendenti; i numeri chiamanti assegnati ai dipendenti non venivano registrati, mentre i numeri chiamati venivano registrati, ma con oscuramento delle ultime tre cifre, conservandosi in chiaro solo la documentazione delle chiamate relative a numerazioni assegnate a società esterne; i dati di traffico erano conservati "per non più di 180 giorni", per esigenze di documentazione in caso di contestazione della fatturazione da parte delle società esterne; pur essendo disponibile nell'applicativo *Blue's* la funzione "*alert*", che consentiva l'invio, ad un indirizzo di posta elettronica prescelto dal datore di lavoro, di un messaggio di avviso ogni qual volta il sistema avesse rilevato una chiamata telefonica verso numeri esterni preindicati come da monitorare, la stessa funzione non era stata mai attivata.

4.1 Il motivo è infondato.

Si deve rilevare che l'affermazione del ricorrente, secondo cui i numeri del traffico telefonico relativo ai dipendenti non erano conservati e che, nel conservare documentazione dei numeri telefonici chiamati dai propri dipendenti, ne fossero occultate le ultime tre cifre, è smentita dalle risultanze processuali. Il Giudice di merito dà atto del contrario: sarebbe stato preciso onere della parte indicare specificamente su quale atto processuale la sua affermazione potesse trovare fondamento.

Non è pertinente l'obiezione secondo la quale la prolungata conservazione dei dati relativi al traffico sarebbe stata prevista solo per il caso di eventuali contestazioni della fatturazione da parte dei soggetti terzi: non si vede, infatti, in qual modo il soddisfacimento di questa esigenza dovesse comportare la conservazione dei dati relativi al traffico telefonico anche dei dipendenti e per un prolungato periodo di tempo.

In ordine alla funzione "alert", prevista dall'applicativo *Blue's*, il Giudice di merito, implicitamente e plausibilmente, l'ha ritenuta lesiva dei diritti dei lavoratori, in assenza del positivo espletamento delle procedure di cui all'art. 4, secondo comma, dello Statuto dei lavoratori, ed è corretta, pertanto, la richiesta del Garante di escluderla, a prescindere dal fatto che essa fosse stata concretamente utilizzata.

Si deve dare continuità all'orientamento espresso da questa Corte a proposito del controllo del traffico telefonico dei dipendenti, attuato mediante il sistema *Blue's*, che si sosteneva essere giustificato (anche) per esigenze di contrasto alle attività illecite che avrebbero potuto essere poste in essere dai lavoratori a danno del datore di lavoro e, quindi, estraneo all'ambito applicativo dell'art. 4 della legge n. 300 del 1970, trattandosi asseritamente di una modalità di controllo difensivo lecito. A queste obiezioni la Cassazione ha replicato, affermando che "l'effettività del divieto di controllo a distanza dell'attività dei lavoratori richiede che anche per i cd. controlli difensivi trovino applicazione le garanzie del citato art. 4, secondo comma, e che, comunque, quest'ultimi, così come la altre fattispecie di controllo ivi previste, non si traducano in forme surrettizie di controllo a distanza dell'attività lavorativa dei lavoratori. Se per l'esigenza di evitare attività illecite

o per motivi organizzativi o produttivi, possono essere installati impianti ed apparecchiature di controllo che rilevino dati relativi anche alla attività lavorativa dei lavoratori, la previsione che siano osservate le garanzie procedurali di cui all'art. 4, comma 2, non consente che attraverso tali strumenti, sia pure adottati in esito alla concertazione con le r.s.a., si possa porre in essere, anche se quale conseguenza mediata, un controllo a distanza dei lavoratori che, giova ribadirlo, è vietato dall'art. 4, comma 1, cit. Il divieto di controlli a distanza ex art. 4, della legge n. 300 del 1970, implica, dunque, che i controlli difensivi posti in essere con il sistema informatico *Blue's* 2002, ricadono nell'ambito della L. n. 300 del 1970, art. 4, comma 2" (Cass. Sez. L, n. 16622 del 2012 cit.).

5. Con il quinto motivo (n. Va) è contestato, ai sensi dell'art. 360, numero 5, c.p.c., l'omesso esame di un fatto decisivo per il giudizio, costituente oggetto di discussione tra le parti, in quanto - contrariamente a quanto contestato dal Garante - il Poligrafico aveva provveduto a rendere conoscibile l'identità degli amministratori di sistema.

5.1 Il motivo è infondato.

Il Giudice di merito ha plausibilmente ritenuto, in senso adesivo alle argomentazioni del Garante, che il Poligrafico, in violazione dell'art. 4, secondo comma, dello Statuto dei lavoratori, aveva utilizzato strumenti elettronici che consentivano la vigilanza a distanza dei dipendenti, senza che fossero state espletate le procedure previste dalla legge. A fronte di tale accertamento, è irrilevante la circostanza che i lavoratori fossero stati

portati a conoscenza dei nominativi degli amministratori abilitati ad accedere al sistema informatico aziendale.

6. In conclusione, il ricorso è rigettato.

Le spese di lite, liquidate in dispositivo, seguono la soccombenza.

P.Q.M.

La Corte rigetta il ricorso; condanna il ricorrente Istituto Poligrafico dello Stato spa, in persona del legale rappresentante pro-tempore, al pagamento delle spese di lite, liquidate in € 7800,00, oltre SPAD.

Si dà atto della sussistenza dei presupposti per il versamento, da parte del ricorrente, dell'ulteriore importo previsto dalla legge a titolo di contributo unificato.

In caso di diffusione del presente provvedimento, omettere le generalità e gli altri dati identificativi.

Così deciso in Roma, il 24 giugno 2016.

Il cons. rel.

Il Presidente

DEPOSITATO
IN CANCELLERIA
IL 19 SET 2016
IL FUNZIONARIO GIUDIZIARIO
Adriana BIANCHI