ria sono offerti da Cerri, *Gli accordi prematrimoniali*, Giuffrè, 2011; Balestra, *Gli accordi in vista del divorzio: la Cassazione conferma il proprio orientamento*, in *Corr. giur.*, 2000, 1023 ss.; Id., *Autonomia negoziale e crisi coniugale: gli accordi in vista della separazione*, in Aa.Vv., *Accordi sulla crisi della famiglia e autonomia coniugale*, a cura di Ruscello, Cedam, 2006, 77 ss.

2. Prenuptial agreements, postnuptial agreements e Eheverträge. Occorre innanzitutto avvertire che la comprensione del fenomeno dei contratti prematrimoniali negli ordinamenti stranieri presuppone una certa conoscenza degli aspetti patrimoniali del diritto di famiglia, per cui si segnala Fusaro, *I rapporti patrimoniali tra coniugi in prospettiva comparatistica*, in *Lezioni di diritto privato europeo*, a cura di Alpa eCapilli, Cedam, 2007, 53 ss.

Per quanto concerne la letteratura straniera ci si limita a brevi cenni.

Merita menzione, in particolare, per la specificità dell'argomento trattato, Bergschneider, *Zur Inhalts kontrolle bei Eheverträgen: das Urteil des Bundesverfassungs gerichts v. 06.02.2001 und seine Konsequenzen für die Praxis*, in *FamRZ*, 2001. Si rinvia inoltre a Boele-Woelki, Miles e Scherpe, *The Future of Family Property in Europe*, Intersentia, 2011; Brambring, *Die Ehevertrags frei heit und ihre Grenzen*, in Hofer-Schwab-Henrich, *From Status to Contract? – Die Bedeutung des Vertrages im europäischen Familien recht*, Gieseking, 2005; Boele-Woelki, Miles e Scherpe, *European Family Law in Action: Volume II: Maintenance Between Former Spouses*, Intersentia, 2003; Pintens, *Ehegüterstände in Europa*, in Lipp-Schumann-Veit, *Die Zugewinngemeinschaft- ein europäisches Modell?*, Universitäts verlag Göttingen, 2009; Scherpe, *Marital Agreements and Private Autonomy in Comparative Perspective*, Hart Publishing, 2012.

Eugenio Tagliasacchi

► CASS. CIV., I sez., 1°.8.2013, n. 18443
Conferma Trib. Palermo, 26.6.2008

Personalità (diritti della) - *Privacy* del lavoratore - Datore di lavoro - Trattamento dei dati personali - Dati personali sensibili - Violazione - Condizioni - Conseguenze (d. legis. 30.6.2003, n. 196, artt. 1-26) (*a*)

Personalità (diritti della) - *Privacy* del lavoratore - Datore di lavoro - Trattamento dei dati personali - Dati personali sensibili - Consenso dell'interessato - Esclusione per esigenze di tutela o difesa di un diritto in giudizio - Condizioni (d. legis. n. 30.6.2003, n. 196 , artt. 23-26) (*b*)

(*a*) **Viola la *privacy* del lavoratore il datore di lavoro che utilizzi i dati attinti dal *computer* di un proprio dipendente in una contestazione disciplinare, per avere indebitamente, durante il rapporto di lavoro, a lungo visitato siti sindacali, di culto e pornografici, trattandosi di dati sensibili idonei a rivelare convinzioni religiose, opinioni sindacali, nonché gusti attinenti alla vita sessuale.**

(*b*) **Le informazioni di natura sensibile possono essere trattate dal datore di lavoro senza il consenso quando il trattamento necessario per far valere o difendere un diritto in sede giudiziaria sia «indispensabile» *ex* art. 26, comma 4°, lett. *c*), del codice della *privacy* (nella specie, relativa al controllo sul *personal computer* di un dipendente, a cui era stato contestato l'accesso illegittimo ad *Internet* durante l'orario lavorativo, anche mediante la consultazione di siti pornografici, la Corte ha ritenuto che dal *computer* fossero stati estratti dati tali da configurare «dati sensibili» perché relativi a convinzioni religiose e politiche nonché alle tendenze sessuali e, pertanto, sebbene i dati personali fossero stati raccolti nell'ambito di controlli infor-**

matici volti a verificare l'esistenza di un comportamento illecito, ne ha sancito l'illegittimità della raccolta).

dal testo:

Il fatto. I motivi. 1. – La s.p.a. M., titolare di una casa di cura, ricorre per cassazione – formulando quattro motivi contro la sentenza del Tribunale di Palermo del 26.6.2008 con la quale è stato respinto il suo ricorso, presentato ai sensi del D.Lgs. n. 196 del 2003, art. 152, contro il provvedimento in data 2.2.2006 con il quale il Garante per la protezione dei dati personali le aveva vietato il trattamento dei dati personali di G.F., proprio dipendente, dal cui computer erano stati estratti dati concernenti l'acceso ad internet, tali da configurare "dati sensibili" perché relativi a convinzioni religiose e politiche nonché alle tendenze sessuali.

Resistono con controricorso G.F. e il Garante della protezione dei dati personali.

2. – La vicenda oggetto del ricorso può essere così riassunta.

G.F. avendo ricevuto dalla casa di cura ricorrente, presso cui prestava servizio come addetto all'accettazione e al banco referti, una contestazione disciplinare relativa ad accessi ad Internet non autorizzati effettuati sul luogo di lavoro, ha chiesto il blocco e la cancellazione dei dati personali che lo riguardano relativi a tali accessi, ai sensi dell'art. 7 Codice.

La s.p.a. Maddalena li aveva documentati producendo numerose pagine – allegate alla contestazione disciplinare – recanti, in particolare, informazioni relative ai "file" temporanei e ai "cookie" originati, sul computer utilizzato dal ricorrente, dalla navigazione in rete avvenuta durante sessioni di lavoro avviate con la password del ricorrente medesimo.

Non avendo ricevuto riscontro, il ricorrente ha presentato ricorso al Garante ai sensi dell'art. 145 e segg. del codice, ritenendo illecito il trattamento.

Il ricorrente ha sostenuto che tra i dati in questione comparivano anche alcune informazioni di carattere sensibile idonee a rivelare, in particolare, convinzioni religiose, opinioni sindacali, nonché gusti e tendenze sessuali posto che numerosi file fanno riferimento a siti Internet a contenuto pornografico. La resistente avrebbe trattato tali dati senza alcun consenso e senza informare preventivamente circa la possibilità di effettuare controlli sui terminali d'ufficio né l'interessato, né il "sindacato interno all'azienda (...), in aperto spregio all'art. 4 dello Statuto dei lavoratori che prevede che tale attività può avvenire solo previo consenso del sindacato o dell'ispettorato del lavoro".

2.1. – Con il provvedimento impugnato dinanzi al Tribunale il Garante ha osservato quanto segue:

"Considerato il collegamento diretto ed univoco che la società ha rappresentato (ai fini della contestazione disciplinare, del licenziamento per giusta causa e della querela sporta) tra la persona del ricorrente e i dati desunti sia dai file temporanei, sia dai cookie prodotti in giudizio, il ricorrente stesso assume la qualità di interessato (art. 4, comma 1, lett. *a*), del Codice, secondo cui è tale la persona fisica (...) cui si riferiscono i dati personali) ed è, pertanto, legittimato ad esercitare i diritti di cui all'art. 7 del Codice e a presentare ricorso al Garante.

Per ciò che concerne il merito va rilevato che la società, per dimostrare un comportamento illecito nel quadro del rapporto di lavoro, ha esperito dettagliati accertamenti in assenza di una previa informativa all'interessato relativa al trattamento dei dati personali, nonché in difformità dall'art. 11 del Codice nella parte in cui prevede che i dati siano trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza rispetto alle finalità perseguite.

Dalla documentazione in atti si evince che la raccolta da parte del datore di lavoro dei dati relativi alle navigazioni in Internet è avvenuta mediante accesso al terminale in uso all'interessato (con copia della cartella relativa a tutte le operazioni poste in essere su tale computer durante le sessioni di lavoro avviate con la sua password, come si desume dalla stringa riportata in apice all'elenco dei file prodotti dalla resistente "c:copiaDocuments and settingsx-y"), anziché mediante accesso a file di backup della cui esistenza il personale della società è informato mediante il manuale della qualità accessibile agli stessi sul proprio terminale.

A parte la circostanza che l'interessato non

era stato, quindi, informato previamente dell'eventualità di tali controlli e del tipo di trattamento che sarebbe stato effettuato, va rilevato sotto altro profilo che non risulta che il ricorrente avesse necessità di accedere ad Internet per svolgere le proprie prestazioni. La resistente avrebbe potuto quindi dimostrare l'illiceità del suo comportamento in rapporto al corretto uso degli strumenti affidati sul luogo di lavoro limitandosi a provare in altro modo l'esistenza di accessi indebiti alla rete e i relativi tempi di collegamento. La società ha invece operato un trattamento diffuso di numerose altre informazioni indicative anche degli specifici contenuti degli accessi dei singoli siti web visitati nel corso delle varie navigazioni, operando – in modo peraltro non trasparente – un trattamento di dati eccedente rispetto alle finalità perseguite.

La raccolta di tali informazioni ha comportato, altresì, il trattamento di alcuni dati sensibili idonei a rivelare convinzioni religiose, opinioni sindacali, nonché gusti attinenti alla vita sessuale (ciò, stante l'elevato numero di informazioni valutate in rapporto ad un lungo arco di tempo, gli specifici contenuti risultanti da alcuni indirizzi web e il contesto unitario in cui il complesso di tali dati è stato valutato), rispetto ai quali la disciplina in materia di dati personali pone peculiari garanzie che non sono state integralmente rispettate nel caso di specie (art. 26 del Codice; aut. gen. del Garante n. 1/2004).

Va infatti tenuto conto che, sebbene i dati personali siano stati raccolti nell'ambito di controlli informatici volti a verificare l'esistenza di un comportamento illecito (che hanno condotto a sporgere una querela, ad una contestazione disciplinare e al licenziamento), le informazioni di natura sensibile possono essere trattate dal datore di lavoro senza il consenso quando il trattamento necessario per far valere o difendere un diritto in sede giudiziaria sia indispensabile (art. 26, comma 4, lett. *c*), del Codice; autorizzazione n. (*OMISSIS*) del Garante). Tale indispensabilità, anche alla luce di quanto precedentemente osservato, non ricorre nel caso di specie.

Inoltre, riguardando anche dati idonei a rivelare lo stato di salute e la vita sessuale, il trattamento era lecito solo per far valere o difendere in giudizio un diritto di rango pari a quello dell'interessato ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile. Anche tale circostanza non ricorre nel caso di specie, nel quale sono stati fatti valere solo diritti legati allo svolgimento del rapporto di lavoro (cfr. art. 26, comma 4, lett. *c*), del Codice; punto 3, lett. *d*), della citata autorizzazione; cfr. Provv. Garante 9 luglio 2003).

Alla luce delle considerazioni sopra esposte e considerato l'art. 11, comma 2, del Codice secondo cui i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati, l'Autorità dispone quindi, ai sensi dell'art. 150, comma 2, del Codice, quale misura a tutela dei diritti dell'interessato, il divieto per la società resistente di trattare ulteriormente i dati personali raccolti nei modi contestati con il ricorso".

2.2. – Il Tribunale, nel rigettare il ricorso della s.p.a. Maddalena ha condiviso le argomentazioni del Garante e, in particolare, ha disatteso l'eccezione di difetto di legittimazione del G., ha ritenuto dati "sensibili" quelli trattati dalla ricorrente e ha accertato, inoltre, che il trattamento era avvenuto senza consenso dell'interessato, fuori dalle ipotesi di cui all'art. 24 del Codice e in modo eccedente.

3.1. – Con il primo motivo di ricorso la ricorrente denuncia violazione e falsa applicazione del D.Lgs. n. 169 del 2003, artt. 4, 141 e 145 art. 12 preleggi, nonché vizio di motivazione.

Deduce che la nozione di interessato ai sensi del D.Lgs. n. 196 del 2003, artt. 4 e 141, alla luce dell'art. 12 preleggi, non può essere interpretata nel senso di conferire legittimazione attiva ai fini del ricorso *ex* art. 145 D.Lgs. cit., anche al soggetto che abbia negato ogni relazione tra sé ed i dati medesimi.

3.2. – Con il secondo motivo la ricorrente denuncia violazione e falsa applicazione del D.Lgs. n. 196 del 2003, art. 4, comma 1, lett. *c*), artt. 12 e 14 preleggi, nonché vizio di motivazione.

Deduce che, ai sensi del D.Lgs. n. 196 del 2003, art. 4 comma 1 lett. *c*), nonché degli artt. 12 e 14 preleggi, la visitazione di differenti siti web ricollegabili a diverse associazioni sindacali non costituisce un dato idoneo a rivelare le opinioni sindacali dell'utente Internet, così come la visitazione di molteplici siti web ricondu-

cibili ad organizzazioni di carattere religioso non costituisce un dato idoneo a rivelare le convinzioni religiose dell'utente Internet. Né, infine, la visitazione di molteplici siti web a contenuto pornografico integra un dato attinente alla "vita sessuale" dell'utente Internet.

3.3. – Con il terzo motivo la ricorrente denuncia violazione e falsa applicazione del D.Lgs. n. 196 del 2003, art. 13, comma 5, lett. *a*), art. 24, comma 1, lett. *a*), *b*) e *g*), art. 26 comma 4, lett. *b*) *c*) e *d*) e art. 40; violazione e falsa applicazione della L. n. 604 del 1966, artt. 1, 2 e 5, come modificata dalla L. n. 108 del 1990, nonché della L. n. 300 del 1970, artt. 7 e 18 (statuto dei lavoratori) nonché delle disposizioni (artt. da 38 a 41) del CCFNL per il personale dipendente delle strutture sanitarie associate AIOP, ARIS e FDG (parte normativa 2002-2005, biennio economico 2002-2003), che disciplina il rapporto, in ordine ai procedimenti disciplinari;violazione e falsa applicazione dell'art. 112 c.p.c.; violazione e falsa applicazione dell'autorizzazione generale del Garante per la protezione dei dati personali n. 1 del 2004 al trattamento dei dati sensibili nei rapporti di lavoro, *sub* 3, lett. A); nonché vizio di motivazione.

Lamenta che la sentenza impugnata abbia omesso di motivare in relazione alla circostanza che il provvedimento autorizzatorio n. 1 del 2004 del Garante per la protezione dei dati personali al trattamento dei dati sensibili nei rapporti di lavoro fosse riferibile all'odierna ricorrente e ne legittimasse il comportamento nonché sulla circostanza che l'attività gestita da La Maddalena S.p.A. fosse destinataria del regime speciale disposto dall'art. 34, comma 4, lett. *b*), in virtù del fatto di essere soggetto accreditato presso il servizio sanitario regionale della Sicilia.

Deduce che – ai sensi del D.Lgs. n. 196 del 2003, art. 13, comma 5, lett. *a*), art. 24, comma 1, lett. *a*), *b*) e *g*), art. 26, comma 4, lett. *b*), *c*) e *d*), e art. 40; della L. n. 604 del 1966, artt. 1, 2 e 5, come modificata dalla L. n. 108 del 1990, nonché della L. n. 300 del 1970, artt. 7 e 18 (Statuto dei lavoratori), nonché delle disposizioni (artt. da 38 a 41) del CCNL per il personale dipendente delle strutture sanitarie associate Aiop, Aris e Fdg (parte normativa 2002-2005, biennio economico 2002-2003) e dell'Autorizzazione Generale del Garante per la Protezione dei Dati Personali n. 1 del 2004 al trattamento dei dati sensibili nei rapporti di lavoro – il rispetto degli obblighi imposti al datore di lavoro per procedere alla legittima risoluzione del rapporto esclude la necessità della previa acquisizione del consenso dell'interessato".

La ricorrente, inoltre, deduce che la sentenza impugnata è viziata – *ex* art. 112 c.p.c. – nella parte in cui ha omesso di pronunciarsi sull'idoneità degli obblighi imposti dalla legge e dal CCNL per il licenziamento disciplinare, a sollevare il datore di lavoro dall'obbligo di previa acquisizione del consenso al trattamento di dati riferibili all'interessato-prestatore di lavoro.

Deduce, ancora, la violazione del D.Lgs. n. 196 del 2003, art. 40, perché il tribunale ha qualificato come trattamento illecito di dati una condotta che, ai sensi dell'autorizzazione generale, costituisce trattamento lecito.

Deduce, infine, l'erroneità della sentenza nella parte in cui non proporziona il giudizio sulla congruenza, proporzionalità e non eccedenza del trattamento alle finalità che, con esso, il titolare ha voluto (ed aveva l'obbligo di) perseguire.

3.4. – Con il quarto motivo la ricorrente denuncia violazione e falsa applicazione dell'art. 112 c.p.c. (art. 360, n. 3); nullità della sentenza *ex* art. 156 c.p.c. (art. 360 c.p.c., n. 4).

Deduce che l'art. 112 c.p.c., impone che la sentenza contenga, anche in dispositivo, le conclusioni circa l'accoglimento o il rigetto, già espressamente contenute nella motivazione, in relazione a ciascuna delle domande proposte nel giudizio dalla stessa definito e lamenta la nullità della sentenza perché non contiene, in dispositivo, alcuna menzione del rigetto della domanda di danni formulata dal G.

4.1. – Ai sensi del D.Lgs. n. 169 del 2003, art. 4 lett. *i*), è "interessato", la persona fisica cui si riferiscono i dati personali oggetto di un determinato trattamento. Avendo il G. ricevuto dalla casa di cura ricorrente una contestazione disciplinare relativa ad accessi ad Internet non autorizzati effettuati sul luogo di lavoro, egli era certamente legittimato, ai sensi dell'art. 7 Codice, a chiedere il blocco e la cancellazione dei dati personali che gli venivano imputati.

Il tribunale, dunque, ha correttamente applicato i principi espressi dalla giurisprudenza di questa Corte secondo la quale "ai fini del trattamento dei dati personali, come disciplinato dalla L. 31 dicembre 1996, n. 675 (e quindi dal D.Lgs. 30 giugno 2003, n. 196), e dell'esperibilità della tutela predisposta dall'art. 1 e segg., perché una persona assuma la qualità di 'interessato' è necessario che i dati di cui si controverta riguardino la persona fisica o la persona giuridica o l'ente o l'associazione che si dolga proprio del loro trattamento, non essendo richiesto che i dati appartengano, con certezza, alla persona che si duole delle operazioni compiute su di essi, atteso che quel che rileva è la loro attribuzione o la loro esclusione rispetto a colui che, al riguardo, accampi un diritto (alla titolarità ovvero all'estraneità dei dati)". Pertanto, anche l'inesatto trattamento dei dati consente di invocare, presso la competente autorità di garanzia la tutela apprestata dalla legge, il cui disegno è funzionale alla difesa della persona e dei suoi fondamentali diritti e tende ad impedire che l'uso, astrattamente legittimo, del dato personale avvenga con modalità tali da renderlo lesivo di quei diritti: qualora, perciò, si contesti l'attribuzione alla propria persona di determinate immagini, non ci si spoglia, per ciò stesso, della qualità di "interessato", perché proprio il fatto che il soggetto intenda escludere l'attribuzione a sé di quei dati iconici comporta che egli abbia assunto, a ragione, quella qualificazione e, in forza di essa, possa chiedere (nella specie, al Garante e quindi al Tribunale) l'adozione di provvedimenti (Sez. 1, Sentenza n. 14390 del 08/07/2005).

Talché il primo motivo è infondato.

4.2. – Il D.Lgs. n. 196/2003 definisce all'art. 4, comma 1, lett. *d*) i "dati sensibili" come quei "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". In dottrina, in proposito, si è rilevato che la consapevolezza dei rischi insiti in un atteggiamento improntato ad un'eccessiva restrizione delle ipotesi in cui la tutela rafforzata debba essere riconosciuta, è ben chiara nella mente del legislatore, che ha adottato, sin dal 1996, una definizione di dato sensibile più ampia rispetto a quella comunitaria, posto che,diversamente dall'art. 8 della Direttiva 95/46/CE, l'art. 4, comma 1, lett. *d*) del codice (così come il precedente art. 22, comma 1) utilizza la formula "dato idoneo a rivelare", piuttosto che quella di "dato che rivela", estendendosi l'attributo della sensibilità anche a quelle informazioni che, seppur di per sé neutre, possano sulla scorta di un procedimento logico condurre a rivelare dati peculiari, in relazione al particolare contesto in cui avviene il trattamento.

Allo stesso fine è stato valorizzato il riferimento alle "convinzioni di altro genere", contenuto nella norma interna ma assente in quella europea, ritenendosi che con esso si è inteso costituire una clausola di chiusura per qualsiasi informazione che identifichi un credo, una convinzione o un'opinione personale. Credo, convinzione o opinione personale indubbiamente desumibili anche dai dati relativi all'accesso a siti web ricollegabili a diverse associazioni sindacali ovvero riconducibili ad organizzazioni di carattere religioso da parte dell'utente Internet.

Invero, già da tempo il competente gruppo di lavoro della Commissione Europea – dopo avere ribadito che "un principio fondamentale in materia di protezione dei dati (vedi articoli 6(1) (c) e 7 della direttiva 95/46/CE) è che i dati personali raccolti in qualsiasi situazione debbano limitarsi a quanto è strettamente necessario e attinente alla finalità in questione" e che "ogni tipo d'informazione personale costituisce una minaccia potenziale alla riservatezza di una persona ed è quindi necessario fare in modo che, quando tali informazioni vengono raccolte, ciò avvenga per una finalità legittima e che la quantità d'informazioni raccolte sia limitata al minimo indispensabile" – ha evidenziato che i rischi alla riservatezza personale risiedono non solo nell'esistenza di grandi quantitativi di dati personali su Internet, ma anche nello sviluppo del software capace di esplorare la rete e mettere assieme tutti i dati disponibili relativi a una determinata persona, essendo possibile "compilare una biografia dettagliata di una persona", "...utilizzando tale software e sfruttando le informazioni provenienti da tutti i gruppi di discussione a cui la persona ha par-

tecipato" (Commissione Europea, Raccomandazione 3/97, Anonimato su Internet, 3 dicembre 1997).

Quanto al profilo della censura relativo alla vita sessuale, va evidenziato che "pornografia" è la "trattazione o rappresentazione (attraverso scritti, disegni, fotografie, film, spettacoli, ecc.) di soggetti o immagini ritenuti osceni, fatta con lo scopo di stimolare eroticamente il lettore o lo spettatore" e l'erotismo è "l'insieme delle manifestazioni dell'istinto sessuale sia sul piano psicologico e affettivo sia su quello comportamentale". Secondo le sezioni penali di questa Corte "la pornografia è compresa nel più ampio concetto di oscenità, e si identifica con la descrizione o illustrazione di soggetti erotici, mediante scritti, disegni, discorsi, fotografie, ecc, che siano idonei a far venir meno il senso della continenza sessuale e offendano il pudore per la loro manifesta licenziosità" (Cass. Sez. 3^, n. 1197 del 6.11.1970, Bianco, mass. 116647).

In sessuologia si afferma che nell'uomo la sessualità appare strettamente legata a fattori di ordine psicologico, culturale e sociale che in ogni individuo prevalgono sui fattori biologici, costituendo la base della cosiddetta vita sessuale o comportamento sessuale, teso non solo alla finalità riproduttiva ma anche alla ricerca del piacere.

Questa Corte (in sede penale) ha già avuto modo di precisare che la circostanza che oggetto di tutela da parte del D.Lgs. n. 196 del 2003 "non siano solo i gusti sessuali di un individuo (astrattamente e genericamente considerati), ma, anche, le concrete scelte che, in questo campo, il soggetto va ad operare, è chiaramente evincibile dalla stessa lettera del citato art. 4, laddove (comma 1, lett. *d*)) definisce i dati sensibili con riferimento ai dati personali idonei a rivelare lo stato di salute e la vita sessuale (non semplicemente le tendenze o le aspirazioni in tale campo)" (Sez. 5 penale, Sentenza n. 44940 del 2011).

Pertanto, è indubbio che sono dati personali idonei a rivelare la vita sessuale – "da intendersi come complesso delle modalità di soddisfacimento degli appetiti sessuali di una persona" (Sez. 5 penale, Sentenza n. 46454 del 2008) – quelli relativi alla "navigazione" in internet con accesso a siti pornografici.

Il secondo motivo, dunque, è infondato.

4.3. – Quanto alle numerose censure compendiate nel terzo motivo va evidenziato che ai sensi del D.Lgs. n. 196 del 2003, art. 11, i dati oggetto del trattamento devono – tra l'altro – essere "pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati" e la stessa autorizzazione n. 1 del 2004 del Garante, invocata a più riprese dalla ricorrente, precisa (al par. 5) che "fermi restando gli obblighi previsti dagli artt. 11 e 14 del Codice, nonché dall'art. 31 e segg. Codice e dall'Allegato B) al medesimo Codice, il trattamento dei dati sensibili deve essere effettuato unicamente con operazioni, nonché con logiche e mediante forme di organizzazione dei dati strettamente indispensabili in rapporto ai sopra indicati obblighi, compiti o finalità".

Ciò posto, va rilevato che con congrua e logica motivazione, anche mediante illustrazione dei corretti metodi di ricerca e neutralizzazione di virus informatici, il Tribunale ha accertato in fatto che il trattamento dei dati sensibili era avvenuto in modo eccedente rispetto alla finalità del medesimo. In particolare, sempre con accertamento in fatto incensurabile in questa sede, il tribunale ha condiviso le argomentazioni del Garante secondo cui la ricorrente avrebbe potuto dimostrare l'illiceità del comportamento del dipendente, in rapporto al corretto uso degli strumenti affidati sul luogo di lavoro, limitandosi a provare in altro modo l'esistenza di accessi indebiti alla rete e i relativi tempi di collegamento.

Essa, per contro, ha operato un trattamento diffuso di numerose altre informazioni indicative anche degli specifici "contenuti" degli accessi dei singoli siti web visitati nel corso delle varie navigazioni, operando – in modo peraltro non trasparente – un trattamento di dati eccedente rispetto alle finalità perseguite, tenuto conto che, sebbene i dati personali siano stati raccolti nell'ambito di controlli informatici volti a verificare l'esistenza di un comportamento illecito, le informazioni di natura sensibile possono essere trattate dal datore di lavoro senza il consenso quando il trattamento necessario per far valere o difendere un diritto in sede giudiziaria sia "indispensabile" e tale indispensabilità, non ricorre nel caso di specie.

Infine, pure con accertamento in fatto adeguatamente giustificato, il giudice del merito ha accertato che la "scoperta" del virus informatico è stata la "conseguenza" del controllo operato sul computer e non la ragione del controllo.

Per converso, le censure di cui al terzo motivo sono del tutto aspecifiche e generiche rispetto alla menzionata ratio decidendi, sì che il motivo è inammissibile.

4.4. – È del pari inammissibile, infine, il quarto motivo per evidente carenza di interesse in quanto lamenta l'omessa pronuncia su domanda (non accolta) formulata dalla controparte.

Il ricorso, pertanto, deve essere rigettato.

Le spese del giudizio di legittimità – liquidate in dispositivo – seguono la soccombenza. (*Omissis*)

[Didone *Estensore*. – M. S.p.A. (avv. Fortuna) – G.F. (avv. Sigillò) e Garante per la Protezione dei dati personali (Avv. gen. dello Stato)]

Nota di commento: «*I "controlli tecnologici" del datore di lavoro tra necessità e proporzionalità. Chiare indicazioni lavoristiche dalla prima Sezione civile*» [★]

I. **Il caso**

Con la sentenza in commento la prima sezione civile della Corte di Cassazione fornisce una serie di chiarimenti sistematici della massima rilevanza, suscettibili di implicanze assai rilevanti nell'ambito del dibattito lavoristico sui cc.dd. controlli «tecnologici» del datore di lavoro.

Il caso è paradigmatico, quasi scolastico. Un tale, addetto all'accettazione e al banco referti di una casa di cura, riceve una contestazione disciplinare relativa ad accessi ad *Internet* non autorizzati, effettuati sul luogo di lavoro. Il datore aveva documentato tali accessi accedendo al *computer* in uso all'interessato ed effettuando una copia della cartella relativa a tutte le operazioni poste in essere su tale *computer* durante le sessioni di lavoro avviate dal lavoratore con la propria *password*. La documentazione così ottenuta comprendeva informazioni anche di carattere sensibile atteso che numerosi *files* facevano riferimento a siti *Internet* alcuni di carattere religioso e altri, molteplici, di contenuto pornografico. Il trattamento di tali dati era avvenuto senza alcun consenso, senza che il datore di lavoro avesse informato preventivamente il lavoratore e senza attivare la procedura codeterminativa di cui all'art. 4 St. lav.

La sentenza, nel compendiare i diversi principi che governano la materia relativa alla tutela della privatezza, afferma che, nel caso di specie, il datore di lavoro avrebbe potuto perseguire le proprie finalità (consistenti precipuamente nella protezione del sistema informatico rispetto al rischio di *virus* ed alla verifica circa il corretto adempimento dell'obbligazione di lavoro) limitandosi a provare in altro modo l'esistenza di accessi indebiti alla rete e i relativi tempi di collegamento. Partendo da questa considerazione la Corte perviene all'affermazione del *carattere eccedente del trattamento dei dati (sensibili) rispetto alla finalità del trattamento*. La sentenza si segnala dunque per la chiara e condivisibile *valorizzazione dei principi di necessità, liceità, pertinenza e non eccedenza quali criteri di governo delle regole in materia di privatezza*.

II. **Le questioni**

1. *Accessi ad* Internet *e potere di controllo del datore di lavoro: l'*impasse *del dibattito lavoristico.* La Sezione lavoro della Corte di Cassazione è intervenuta, recentemente, sulla nota vicenda del controllo sugli accessi ad *Internet* realizzato attraverso appositi programmi informatici, confermando l'impostazione seguita nei precedenti gradi di giudizio. La Corte ha ritenuto che «*i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi ad Internet sono strumenti di controllo allorquando consentono al datore di lavoro di controllare a distanza e in via continuativa l'attività lavorativa. In tal caso, la loro installazione è soggetta alla disciplina di cui all'art. 4 l. n. 300/70. La violazione di tale disciplina rende inutilizzabili i dati acquisiti per eventuali sanzioni disciplinari*» (così Cass., 23.2.2010, n. 4375, *infra*, sez. III).

La quinta Sezione penale, invece, allineandosi ad un proprio consolidato orientamento (cfr., in particolare, Cass. pen., 8.10.1985, e Cass. pen., 28.5.1985. Per un orientamento difforme cfr. Cass., 16.10.2009, n. 40199, tutte *infra*, sez. III), ha confermato la condanna per appropriazione indebita inflitta ad una commessa sorpresa da una telecamera mentre sottraeva del denaro dalla cassa dell'esercizio commerciale, ritenendo che «*gli artt. 4 e 38 dello statuto dei lavoratori implicano l'accordo sindacale a fini di riservatezza dei lavoratori nello svolgimento dell'attività lavorativa, ma non implicano il divieto dei c.d. controlli difensivi del patrimonio aziendale da*

[★] **Contributo pubblicato in base a *referee*.**

azioni delittuose da chiunque provenienti» (Cass. pen., 1°.6.2010, n. 20722, *infra*, sez. III).

La tematica dei cc.dd. «controlli difensivi» involge questioni di principio della massima rilevanza, pratica e teorica; in particolare essa pone un laceranteo dilemma circa i confini del diritto alla riservatezza garantito ai lavoratori dal nostro ordinamento, e segnatamente dal combinato disposto degli artt. 4 e 8 St. lav., 41 Cost. e del c.d. codice della *privacy*.

Una interessante sentenza di merito ha lucidamente sintetizzato la problematica attraverso la posizione dell'affermazione, pure dubitativa, secondo cui la *privacy* è «*bene troppo prezioso, anche per le sue implicazioni di ordine costituzionale, 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*» (Trib. Torino, 8.1.2008, *infra*, sez. III). Il Tribunale di Torino, con riferimento ad una fattispecie analoga a quella decisa dalla Sezione lavoro nei primi mesi del 2010, ha affermato che non è consentito ad un lavoratore che abbia utilizzato abusivamente strumentazioni di proprietà aziendale «*invocare il diritto alla* privacy*, che sarebbe non già la tutela di un diritto costituzionale, ma diverrebbe la tutela dell'abuso, destinata ad impedire i controlli – essi sì legittimi – del datore di lavoro su telefonate e SMS del cui costo si è fatto economicamente carico (o meglio ha dovuto farsi carico) per fatto imputabile esclusivamente al dipendente*», il tutto nella prospettiva del divieto di venire *contra factum proprium*, posta dall'art. 1175 cod. civ.

Le preoccupazioni condensate nella motivazione citata richiamano le osservazioni di una dottrina assai autorevole, che, già nel 1986, evidenziava che «la finalità difensiva del controllo esclude in radice che quest'ultimo assuma il carattere di strumento di manipolazione (attraverso l'esercizio di una coazione psicologica) della condotta del lavoratore; salvo che non si voglia paradossalmente giungere ad affermare che il legislatore abbia voluto ritenere meritevole di tutela la possibilità del lavoratore di determinarsi liberamente alla commissione di un illecito» (così Liso, 377; si veda anche Dell'Olio, 487 ss.; Fezzi, 380 ss.; Veneziani, 79 ss.; Romei, 67 ss.; Bellavista, 197 ss.; Gentile, 477 ss., tutti *infra*, sez. IV).

L'approccio della giurisprudenza più recente in relazione al problema dei controlli tecnologici poggia sull'affermazione, già contenuta in una sentenza del 2007 (Cass., 17.7.2007, n. 15892, *infra*, sez. III), in base alla quale «*la 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, per cui tale esigenza non consente di espungere dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso*» (Cass., 23.2.2010, n. 4375, cit.).

La giurisprudenza della Sezione lavoro sembra dunque consolidarsi nel senso di limitare l'ambito di operatività dei c.d. controlli difensivi al solo profilo relativo all'accertamento di condotte illecite del lavoratore. La precisazione concettuale sopra richiamata compendia invero il principio, incidentalmente affermato dalla Corte di legittimità nel 2002, a mente del quale «*ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 legge n. 300 del 1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aule riservate o gli apparecchi di rilevazione di telefonate ingiustificate*» (Cass., 3.4.2002, n. 4746. In senso analogo si veda anche Min. lav., 6.6.2006, entrambe *infra*, sez. III).

Le più recenti sentenze relative al caso dei programmi «*Super Scout*» e «*Blues*» (Cass., 23.2.2010, n. 4375, cit. e Cass., 1°.10.2012, n. 16622, *infra*, sez. III) segnano una battuta di arresto nell'evoluzione giurisprudenziale in materia di «controlli difensivi», la cui categoria concettuale viene sostanzialmente ricondotta a quei controlli esclusivamente indirizzati alla prevenzione e/o all'accertamento di condotte illecite dei dipendenti, esclusi, peraltro tutti quei casi (che sono però la maggioranza), in cui il dispositivo di monitoraggio consenta di controllare anche altri aspetti (leciti) del comportamento del lavoratore: in questi casi si ricade ancora una volta nell'ambito di applicazione dell'art. 4, comma 2°, St. lav. (cfr., fra gli altri, De Luca Tamajo, 30; Nogler, 14; Aimo, 124; Bellavista; Carinci, 218 ss.; Perone, 252, tutti *infra*, sez. IV). Questa lettura sembra obliterare in parte quell'opinione dottrinaria secondo la quale «non sembrano rientrare [...] nell'articolo 4 quei controlli (potrebbero chiamarsi difensivi) che sono volti unicamente ad assicurare il rispetto di una ben determinata regola che impone un comportamento omissivo, oppure a stimolare nei lavoratori una attitudine di auto contenimento nell'uso di determinati beni produttivi» (così Liso, 374).

I due nodi interpretativi che hanno maggiormente interessato i giudici nazionali concernono, in primo luogo, la questione circa l'applicabilità o no dell'art. 4 St. lav. al monitoraggio degli accessi ad *Inter-*

net e, in secondo luogo, l'esatta delimitazione della categoria dei cc.dd. controlli difensivi, alcuni dei quali addirittura ritenuti immuni da qualsivoglia limite procedimentale.

Una giurisprudenza pressoché isolata aveva, invero, mostrato un atteggiamento di apertura, sbilanciato più sulle esigenze organizzative del datore di lavoro che non sulle garanzie di libertà e privatezza dei lavoratori, in qualche modo non interessandosi troppo dell'art. 4 St. lav.

In questo senso si era espresso il Tribunale di Milano, con una sentenza delgiugno 2001, secondo cui «*il comportamento del lavoratore, consistito in un collegamento quotidiano alla rete Internet per più ore al giorno in assenza di effettive necessità lavorative, costituisce un rilevante inadempimento degli obblighi di diligenza e integra una giusta causa di licenziamento; il datore di lavoro può fornire la prova dei collegamenti contestati, oltre che mediante testimoni, anche attraverso l'allegazione dei dati forniti dal* provider *circa gli accessi alla rete provenienti da ogni singola postazione di lavoro*» (Trib. Milano, 8.6.2001, *infra*, sez. III).

Sotto il profilo lavoristico, dunque, il Tribunale aveva ritenuto che l'abuso di *Internet* da parte di un dipendente costituisse un rilevante inadempimento degli obblighi contrattuali, come tale integrante una giusta causa di licenziamento, con possibilità, per il datore di lavoro, di provare l'utilizzo vietato attraverso i dati registrati dal provider, ossia l'impresa informatica che fornisce l'accesso a *Internet* e si occupa della gestione dei servizi per il cliente, senza che tale controllo – e qui sta il passaggio fondamentale della decisione – necessiti della procedura codeterminativa di cui all'art. 4 St. lav.

Questa pronuncia è stata aspramente criticata dalla dottrina, secondo la quale, ciò che desta maggiore sorpresa nella motivazione di questa sentenza, è il fatto che nel percorso argomentativo del giudice non vi sia stata alcuna verifica della legittimità del controllo tecnico così svolto alla luce dell'art. 4 St. lav. (cfr. Bellavista, 65; Bulgarini d'Elci, 1068, secondo cui il citato aspetto della decisione genera pesanti preoccupazioni, tutti *infra*, sez. IV).

In totale contrasto con l'atteggiamento assunto dall'isolata pronuncia sopra richiamata si pone l'orientamento, recentemente confermato dalla Suprema Corte, volto a privilegiare in modo più rigoroso le istanze di libertà e dignità dei lavoratori, spostando maggiormente verso questa direzione lo sforzo interpretativo finalizzato al raggiungimento di un punto di equilibrio armonico tra le opposte esigenze di cui all'art. 41 Cost.

I controlli, per essere genuinamente «difensivi», devono, in primo luogo, essere diretti ad accertare condotte illecite del lavoratore a tutela di beni estranei al rapporto di lavoro(cfr. da ultimo Cass., 23.2.2012, n. 2722, Cass., 17.7.2007, n. 15982, entrambe citt.).

Come messo in evidenza dalla sentenza n. 15982 del luglio 2007, l'insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti «non consente di espungere dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso ove la sorveglianza venga effettuata mediante strumenti che presentano quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro».

Al fine di uscire dall'ambito di applicazione dell'art. 4 St. lav. non risulta dunque sufficiente la pura e semplice natura difensiva del controllo, in quanto la norma in questione, nel legittimare il controllo per esigenze di sicurezza, attraverso la procedura codeterminativa, include nel proprio perimetro precettivo anche una parte dei controlli difensivi, e segnatamente quelli diretti sì ad accertare condotte illecite dei lavoratori, ma quando queste ultime riguardino l'esatto adempimento della prestazione di lavoro.

I controlli, allora, per essere considerati veramente difensivi, non devono concretarsi in un sistema preordinato a vigilare a distanza l'esecuzione dell'attività lavorativa, ma in una verifica effettuata a posteriori sul sistema informatico aziendale, che, presentando un'intrinseca idoneità alla registrazione e quindi alla verifica a ritroso delle attività svolte, occasionalmente può rilevare condotte illecite del dipendente (cfr. App. L'Aquila, 14.12.2006, che conferma Trib. Teramo, 12.5.2006, tutte *infra*, sez. III).

La *ratio* dei divieti di cui all'art. 4 St. lav., quello intenzionale di cui al comma 1º e quello «preterintenzionale» di cui al comma 2º, è quella volta a far sì, come si deduce dalla già richiamata Relazione del Ministro dell'epoca, che la vigilanza sul lavoro sia mantenuta in una dimensione «umana» e quindi non sia esasperata dall'uso di tecnologie che la possano rendere continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro.

Ecco che allora il divieto preterintenzionale è destinato a valere per quei programmi aventi proprio la finalità di monitorare gli accessi ad *Internet* conferendo *ex ante* al datore di lavoro l'intrinseca possibilità di vigilare in tempo reale l'adempimento della prestazione lavorativa, in modo appunto continuo e anelastico.

Ben diverso è invece il caso del datore di lavoro che esegua la pulizia del sistema informatico a seguito della contrazione di un virus e accerti in questa verifica, condotta *ex post* e senza alcuna finalizzazione che non sia il ripristino del sistema, l'illecita condotta del lavoratore (al quale evidentemente risale grazie al sistema di autenticazione informatica): in questo caso viene condotto un controllo tecnico molto puntuale, non di certo continuo e anelastico, scongiurando il rischio di eccessiva compressione della libertà e dignità del lavoratore, comunque destinate ad affievolirsi rispetto alla necessità di salvaguardare, nella specifica ipotesi, il patrimonio aziendale.

Tali circostanze sono state prese in seria considerazione dalla Corte di Cassazione con una fondamentale sentenza del febbraio 2012 (Cass., 23.2.2012, n. 2722, *infra*, sez. III), che costituisce, ad oggi, il momento di sintesi più equilibrato, a parere di chi scrive, nella materia qui oggetto di studio. Nella specie, una Banca aveva licenziato per giusta causa un proprio dipendente accusato di aver divulgato a mezzo di messaggi di posta elettronica, diretti ad estranei, notizie riservate concernenti un cliente dell'Istituto e di aver posto in essere, grazie alle notizie in questione, operazioni finanziarie da cui aveva tratto vantaggio personale.

La Banca aveva acquisito il testo dei messaggi di posta elettronica scambiati dal dipendente con soggetti estranei, *ex post*, ovvero dopo l'attuazione del comportamento addebitato al dipendente, quando erano emersi elementi di fatto tali da raccomandare l'avvio di un'indagine «retrospettiva».

La Corte di Cassazione ha precisato che «*in questo caso entrava in gioco il diritto del datore di lavoro di tutelare il proprio patrimonio, che era costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico*».

I risultati del controllo difensivo così attuato, in ogni caso, possono essere utilizzati soltanto in modo proporzionato e pertinente rispetto alla natura stessa del controllo effettuato.

Il datore di lavoro, conseguentemente, dovrebbe potere, ad esempio, sanzionare disciplinarmente, o esperire una richiesta risarcitoria nei confronti del dipendente che ha danneggiato il sistema informatico aziendale a causa dell'utilizzo di Internet per motivi personali, ma non contestare al lavoratore l'assenza della prestazione lavorativa per il tempo corrispondente ai vari collegamenti, trattandosi quest'ultimo di un utilizzo sproporzionato rispetto alla *ratio* del controllo difensivo e che richiede la procedura di cui all'art. 4, comma 2°, St. lav.

Nel caso indicato, peraltro, si dovrebbe arrivare al punto di riconoscere al datore di lavoro la possibilità di accertare quali siti specificamente abbia visitato il dipendente, al fine di accertare se il virus sia stato contratto in modo incolpevole attraverso la navigazione in siti con finalità professionale oppure in siti totalmente esorbitanti dalla predetta finalità.

La giurisprudenza più recente ha, dunque, accantonato l'affermazione giurisprudenziale secondo cui devono ritenersi fuori dall'ambito di applicazione dell'art. 4 St. lav. i controlli diretti ad accertare condotte illecite del lavoratore, così testualmente «correggendo l'impostazione di Cass. n. 4746 del 2002».

La Sezione lavoro, invero, intervenendo in ultima istanza sulla nota vicenda del controllo sugli accessi ad Internet realizzato attraverso apposito programma informatico (nel caso di specie denominato «Blue's 2002», del tutto analogo ad altri programmi, denominati «Super Scout» o «Squid». Il programma «Super Scout» è stato oggetto della sentenza di Cassazione n. 4378 del 2010, mentre il programma «Squid» è oggetto di un interessante provvedimento del Garante Privacy del 2.4.2009, *infra*, sez. III), ritiene che i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi ad *Internet* sono strumenti di controllo allorquando consentono al datore di lavoro di controllare a distanza e in via continuativa l'attività lavorativa. In tal caso, la loro installazione è soggetta alla disciplina di cui all'art. 4 St. lav. la cui violazione rende inutilizzabili i dati acquisiti per eventuali sanzioni disciplinari.

In relazione al profilo sopra richiamato occorre riprendere quanto detto circa il problema delle misure di sicurezza consistenti nell'obbligo di predisposizione di sistemi di autenticazione informatica,

Che un sistema informativo fornisca informazioni sulle operazioni compiute attraverso l'utilizzo del medesimo non solo è tecnologicamente inevitabile (ogni sistema operativo tiene traccia automaticamente dei c.d. *files log*), ma è addirittura necessario atteso che il codice della *privacy* impone, per quanto si è detto, la «profilazione» dell'utente attraverso una procedura di identificazione informatica, funzionale alla protezione dei dati personali e obbligatoria (pena sanzioni amministrative e penali) per il datore di lavoro.

In sintesi, si ribadisce che il datore di lavoro deve costituire il sistema informativo in modo tale che sia sempre possibile all'amministratore di sistema controllare chi abbia effettuato certe operazioni di trattamento dei dati personali (si veda l'allegato B al codice della *privacy*).

Questo controllo «obbligato» non si ritiene oggetto di procedimentalizzazione *ex* art. 4 St. lav. Diverso è il caso in cui il datore di lavoro intenda fare un uso ulteriore (finalizzato, evidentemente, alla tutela dell'interesse creditorio al corretto adempimen-

to delle obbligazioni di lavoro) dei dati ottenibili dal sistema informatico. In queste ipotesi l'applicazione dell'art. 4 St. lav. appare necessariamente incontrovertibile.

2. *La sentenza in commento.* La soluzione del problema dei c.d. «controlli difensivi» offerta dalla Corte di Cassazione con la sopra richiamata sentenza n. 2722/2012 ha trovato una conferma nella pronuncia in commento. Questa sentenza offre una lucida rielaborazione dei principi fondamentali in materia di tutela della privatezza nel rapporto di lavoro che vengono, in qualche modo, messi in relazione con la disciplina lavoristica. Leggere questa recente sentenza in combinazione con quella del 2012 consente di valorizzare la fecondità di un approccio al tema della privatezza nel rapporto di lavoro che tenga conto dell'intero modello regolativo, costituito sia dalle norme lavoristiche sia dalle norme di carattere generale contenute nel codice della *privacy*.

La Corte di Cassazione, in particolare, opera una precisa ricostruzione della materia partendo dall'enucleare i principi di liceità, correttezza, pertinenza e non eccedenza del trattamento di dati personali rispetto alle finalità perseguite.

Il principio di necessità, in particolare, ottiene, con la sentenza in annotazione, il riconoscimento della propria rilevanza sistemica anche ai fini lavoristici, naturalmente ove letto ed interpretato in combinazione con gli altri principi fondamentali operanti in materia di trattamento dei dati personali, e si dimostra capace di dispiegare i suoi effetti anche al fine di risolvere la questione, qui esaminata, dei controlli tecnologici.

I dettagli della fattispecie assumono, per quello che si dirà, una rilevanza fondamentale. Le informazioni circa le visitazioni pornografiche del lavoratore erano state acquisite da parte del datore di lavoro, realizzando una copia della cartella con tutte le sessioni di navigazione in rete avviate con la *password* dell'interessato, senza informarlo preventivamente; tali navigazioni erano state documentate attraverso la stampa di informazioni relative a «file» temporanei ed ai «*cookies*» originati sul *computer* utilizzato dal lavoratore stesso dalla navigazione in rete avvenuta durante le sessioni di lavoro predette.

All'esito dell'esame, protrattosi nel tempo, dell'ampio materiale riscontrato, dettagliato e puntuale, attestante una mole estremamente significativa di accessi a siti pornografici, il lavoratore veniva licenziato e querelato.

Il passaggio centrale della motivazione della sentenza qui richiamata è quello in cui viene valorizzata la violazione dei principi di proporzionalità, liceità, trasparenza e necessità.

La Corte, invero, valorizza la circostanza che il lavoratore, addetto all'accettazione e al banco referti, non risulta avesse necessità di accedere ad *Internet* per svolgere le proprie prestazioni e che, ciò nonostante, il datore di lavoro abbia operato un trattamento diffuso di numerose informazioni indicative anche degli specifici contenuti degli accessi dei singoli siti *web* visitati nel corso delle varie navigazioni, operando così, in modo non trasparente, un trattamento eccedente rispetto alle finalità perseguite. Il passaggio centrale della motivazione è quello in cui, gettando un ponte con la sentenza del 2012 relativa al caso dei controlli difensivi, la Corte rileva che, sebbene i dati personali siano stati raccolti nell'ambito di controlli informatici volti a verificare l'esistenza di un controllo illecito, le informazioni, di natura anche sensibile, risultano essere state oggetto di trattamento senza che sussistesse la necessità o comunque l'indispensabilità di far valere o difendere un diritto di rango almeno pari a quello dell'interessato, ovvero consistente in un diritto della personalità o di altro diritto o libertà fondamentale ed inviolabile.

I controlli tecnologici, dunque, sono risultati, nel caso di specie, eccedenti rispetto alla finalità di controllo presupposta dal datore di lavoro, non necessari, né indispensabili, e comunque neppure involgenti una finalità genuinamente difensiva, atteso che, come emerge dalla motivazione della sentenza, la scoperta del virus informatico, posta dal datore di lavoro quale giustificazione in chiave di sicurezza del trattamento, era stata la conseguenza del controllo operato sul computer e non la ragione del controllo.

Il controllo, operato con modalità profondamente invasive e occulte, nasceva dunque con l'intento di sottoporre il dipendente ad una vigilanza sulla prestazione, con una chiara funzione investigativa, evidentemente rientrante nel divieto netto posto dal comma 1° dell'art. 4 St. lav.

Quello che la Corte ha con chiarezza evidenziato è che il tipo di controllo, consistente nella raccolta e documentazione di una mole enorme di dati anche sensibili inerenti il lavoratore, non risultava necessario rispetto allo scopo (finalità) del trattamento.

In questo consiste il criterio di fondo, e chi scrive ritiene che l'indicazione offerta dalla Corte di Cassazione sia perfettamente in linea con una corretta interpretazione del sistema della regolazione attualmente vigente. La Corte, in altri termini, pare confermare l'idea che l'ordinamento possa essere interpretato in chiave sistematica, tenendo conto dell'interazione tra codice della *privacy* e Statuto dei lavoratori, previa verifica, volta per volta, della relazione intercorrente tra interessi confliggenti (si veda in dottrina, da ultimo, Sitzia, 160).

III. **I precedenti**

Sul potere di controllo «tecnologico» del datore di lavoro si vedano Cass., 23.2.2010, n. 4375, in *Lav. e giur.*, 2010, 805 ss., con ampia nota di Dui, *Monitoraggio della posta elettronica e accesso a internet*. Del tutto particolare la pronuncia del Trib. Torino, 8.1.2008, in *Riv. it. dir. lav.*, 2008, II, 845 ss., con nota critica di Imperiali, *Privacy e controllo sull'utilizzo di cellulare e computer aziendali a fini personali: un difficile equilibrio* e in *Arg. dir. lav.*, 2008, II, 1265 ss., con nota adesiva di Iarussi, *L'inutilizzabilità delle prove acquisite a sostegno del licenziamento disciplinare: tra poteri datoriali (e del giudice) e diritto alla riservatezza del lavoratore*.

Per una posizione liberista si veda, isolatamente, Trib. Milano, 8.6.2001, in *D&L Riv. crit. dir. lav.*, 2001, 1067, con nota di Bulgarini d'Elci. Si veda anche Cass., 3.4.2002, n. 4746, in *Mass. giur. lav.*, 2002, 644. Per l'affermazione secondo la quale i controlli, per essere genuinamente «difensivi», devono essere diretti ad accertare condotte illecite del lavoratore a tutela di beni estranei al rapporto di lavoro, si vedano, da ultimo, Cass., 1°.10.2012, n. 16622, in *Foro it.*, 2012, I, 3328; Cass., 23.2.2012, n. 2722, in *Guida al lavoro*, 2012, 11, 30; Cass., 17.7.2007, n. 15892, in *Riv. it. dir. lav.*, 2008, II, 714 ss., con nota di Vallauri e *Riv. giur. lav.*, 2008, II, 358 ss., con nota di Bellavista; App. L'Aquila, 14.12.2006, in *Notiz. giur. lav.*, 2007, 37, che conferma Trib. Teramo, 12.5.2006, *ivi*, 2006, 345. In senso analogo si veda anche Min. lav., 6.6.2006, prot. n. 218, in *Dir. e prat. lav.*, 2006, 2021 ss. e Garante Privacy, provv. 2.4.2009, in *Riv. giur. lav.*, 2010, II, 167 ss.

Nella giurisprudenza penalistica cfr., in particolare, Cass. pen., sez. IV, 8.10.1985, in *Orient. giur. lav.*, 1986, 318 e Cass. pen., sez. II, 28.5.1985, in *Mass. giur. lav.*, 1986, 404, con nota di Papaleoni. Per un orientamento difforme cfr. Cass. pen., 16.10.2009, n. 40199, in *Riv. giur. lav.*, 2010, 275 ss., con nota di Colucci, *L'art. 4 dello statuto dei lavoratori: attualità della norma e procedure ispettive*; Cass. pen., 1°.6.2010, n. 20722, in *Dir. e giust.*, 2010; per un commento si veda Stanchi, *Sui controlli difensivi e l'utilizzabilità della prova di reato*, in *Guida al lavoro*, 2010, n. 26, 15 nonché Conti, *La Sezione lavoro e la Sezione penale della Corte di Cassazione a confronto su controlli a distanza e controlli difensivi*, in *Mass. giur. lav.*, 2010, 561 ss.

IV. **La dottrina**

Sul tema dei controlli difensivi del datore di lavoro la letteratura è piuttosto vasta.

Si vedano, tra i contributi di carattere più generale, relativamente alla ricostruzione del sistema delle fonti ed al rapporto tra la disciplina lavoristica e la normativa in materia di tutela dei dati personali, Sitzia, *Il diritto alla «privatezza» nel rapporto di lavoro tra fonti comunitarie e nazionali*, Cedam, 2013; Aimo, *Privacy, libertà di espressione e rapporto di lavoro*, Jovene, 2003; Bellavista, *Il controllo sui lavoratori*, Giappichelli, 1995.

Più in particolare, con riferimento specifico al problema dei controlli difensivi, si vedanoDe Luca Tamajo, *I controlli sui lavoratori*, ne *I poteri del datore di lavoro nell'impresa*, a cura di Zilio Grandi, Cedam, 2002, 30 ss.; Bulgarini d'Elci, *Licenziamento per abuso di collegamento ad internet e tutela del lavoratore dai controlli a distanza*, in *D&L Riv. crit. dir. lav.*, 2001, 1068; Nogler, *Abuso di telefono aziendale: la decisione su controlli e rimedi*, in *Guida lav.*, 2002, 21, 14 ss.; Gentile, *Innovazioni tecnologiche e art. 4 dello Statuto dei lavoratori*, in *Dir. lav.*, 1996, I, 477 ss.; Romei, *Diritto alla riservatezza del lavoratore e innovazione tecnologica*, in *Quad. dir. lav. e rel. ind.*, 1994, 15, 67 ss.; Bellavista, *Diritti della persona e contratto di lavoro nella elaborazione giurisprudenziale*, *ibidem*, 197 ss.; Veneziani, *L'art. 4 St. lav.: una norma da riformare?*, in *Riv. giur. lav.*, 1991, I, 79 ss.; Ghezzi-Liso, *Computer e controllo dei lavoratori*, in *Giorn. dir. lav. rel. ind.*, 1986, 30, 353 ss.; Dell'Olio, *Art. 4 St. lav. ed elaboratori elettronici*, *Dir. lav.*, 1986, I, 487 ss.; Carinci, *Rivoluzione tecnologica e diritto del lavoro: il rapporto individuale*, *Giorn. dir. lav. rel. ind.*, 1985, 218 ss.; Perone, *Rivoluzione tecnologica e diritto del lavoro. I profili collettivi*, *ibidem*, 252 ss.; Fezzi, *Modificare l'art. 4 St. lav.?*, in *Lav. '80*, 1985, II, 380 ss.

Andrea Sitzia