Diritto e Giustizia
IL QUOTIDIANO DI INFORMAZIONE GIURIDICA

LAVORO

PRIVACY | 18 Febbraio 2006

Controllare la navigazione Internet del lavoratore non è sempre vietato: la ricostruzione "corretta" dell'ultimo provvedimento del Garante

di Alessandro del Ninno

di
Alessandro del Ninno *

L'importante provvedimento del 14 febbraio 2006 - con il quale l'Autorità Garante per la protezione dei dati personali ha accolto il ricorso di un dipendente contro le determinazioni assunte dalla sua azienda a seguito della contestata verifica circa la navigazione non consentita in siti Internet - implica la necessità di effettuare particolari considerazioni, per valutare l'effettiva portata delle indicazioni fornite dall'Autorità Garante.

§ 1 La ricostruzione dei fatti.

In primo luogo la ricostruzione dei fatti. Il lavoratore ha ricevuto dalla casa di cura presso la quale 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. Il lavoratore, che non aveva l'abilitazione ad accedere a Internet in quanto non prevista nel suo mansionario, si era connesso alla rete da un computer aziendale e aveva visitato siti web, tra i quali alcuni a contenuto pornografico. Il datore di lavoro, dopo aver sottoposto a esame i dati del computer, aveva accusato il dipendente di aver consultato siti a contenuto religioso, politico e pornografico, fornendone l'elenco dettagliato in documenti allegati alla contestazione disciplinare e recanti, in particolare, informazioni relative ai "file" temporanei e ai "cookie" originati, sul computer utilizzato dal dipendente, dalla navigazione in rete avvenuta durante sessioni di lavoro avviate con la password del dipendente medesimo.

§ 2 Le argomentazioni a base del ricorso del lavoratore.

Il lavoratore ha sostenuto le seguenti tesi a fondamento del proprio ricorso:

tra i dati trattati dall'azienda nel corso dei controlli 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;
l'azienda 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'articolo 4 dello Statuto dei lavoratori che prevede che tale attività può avvenire solo previo consenso del sindacato o dell'ispettorato del lavoro;
dalla motivazione delle sentenze citate dall'azienda a sostegno delle proprie tesi difensive risulta che nei predetti casi il controllo dei lavoratori è stato considerato lecito in quanto il trattamento di dati personali sarebbe stato breve e non eccedente, ovvero effettuato limitatamente ai tempi di connessione e non ai contenuti;
l'unica password utilizzata dal lavoratore era la "password utente" che consente di avviare la sessione di lavoro sul computer, mentre nessuna password era prevista per entrare nella rete Internet, liberamente accessibile mediante l'icona relativa al browser Explorer di Windows;
nel manuale della qualità dell'azienda non si fa alcun riferimento ai controlli degli accessi ad Internet; comunque non sono stati trattati file di backup poiché dalla stringa contenuta nelle pagine sui dati sulle navigazioni riferite al lavoratore emerge che c'è stata un'operazione manuale di copia della "directory temporary internet files" contenuta in una apposita cartella; analoga operazione sarebbe stata effettuata sulla cronologia delle navigazioni, non riferibile ad un backup automatico;
tra i dati trattati compaiono anche alcune informazioni idonee a rivelare la vita sessuale il cui trattamento, se effettuato senza il consenso scritto dell'interessato, è consentito (articolo 26, comma 4, lett. c) del Codice) solo per far valere in giudizio un diritto "di rango pari a quello dell'interessato"; i diritti fatti valere dall'azienda (risoluzione del rapporto di lavoro, tutela del patrimonio aziendale, asserita finalità sociale perseguita dall'azienda per tutelare la salute del cittadino), non consisterebbero in diritti di pari grado a quelli del lavoratore;
il trattamento effettuato dal datore di lavoro sarebbe pertanto eccedente, dal momento che lo stesso è "durato ad libitum, ovvero almeno dai primi giorni del mese di gennaio 2005".

§ 3 Le argomentazioni difensive dell'azienda.

Nell'argomentare la liceità del proprio operato e dei trattamenti di dati personali del proprio dipendente, l'azienda ha proposto una serie di tesi difensive che possono essere riepilogate come segue (a monte l'azienda ha contestato anche l'irricevibilità formale del ricorso a fronte della affermazione del lavoratore di non aver commesso i fatti contestati):
i relativi trattamenti sarebbero leciti in base alla più recente giurisprudenza sui "controlli difensivi datoriali";
il lavoratore ha effettuato accessi non consentiti - e dunque illeciti - a PC aziendali;
il lavoratore si è appropriato indebitamente del materiale cartaceo utilizzato per stampare i risultati della navigazione;
il lavoratore ha danneggiato la rete aziendale a causa dei virus informatici introdottisi a seguito della navigazione non consentita nei siti Internet contestati (per tutte le vicende sub lettere b, c e d l'azienda ha proposto relativa querela presso le competenti autorità giurisdizionali);
il lavoratore non era stato preventivamente informato di possibili controlli informatici in considerazione del fatto che gli accessi ad Internet, in virtù delle mansioni affidate al lavoratore, non sarebbero dovuti avvenire;
l'azienda è comunque dotata di un manuale della qualità accessibile a tutti i dipendenti della clinica che hanno in uso i terminali aziendali, essendo consultabile dal computer cliccando su apposita icona; il manuale avverte i lavoratori sia della circostanza che per la salvaguardia dei dati si procederà a backup periodici ed all'installazione e manutenzione di opportuni programmi antivirus, sia del fatto che gli elaboratori sono da considerarsi beni aziendali affidati al lavoratore per lo svolgimento delle sue mansioni; ogni utilizzo per fini privati deve essere evitato;
la società non era obbligata a raccogliere il consenso che non è richiesto (articolo 24 del Codice) quando il trattamento, come nel caso di specie, nasce dalla legittima esigenza di far valere i propri diritti, anche ai fini della loro tutela in giudizio. E ciò, sia rispetto al rapporto di lavoro con il lavoratore ed alla sua risoluzione, sia rispetto alla tutela di patrimonio ed attività aziendale,

nonché alla finalità di quest'ultima, rilevante sotto il profilo sociale, operando l'azienda nel campo della sanità accreditata e, quindi, inserita nell'ampio sistema previsto dall'ordinamento per garantire il diritto, di rilevanza costituzionale, alla salute del cittadino;
gli articoli 2, 3 e 4 dello Statuto dei lavoratori non farebbero venire meno il potere dell'imprenditore, ai sensi degli articoli 2086 e 2104 Cc, di controllare direttamente o mediante propria organizzazione gerarchica l'adempimento delle prestazioni cui sono tenuti i lavoratori, e così di accertare eventuali mancanze specifiche dei dipendenti medesimi già commesse o in corso di esecuzione; per poter applicare il divieto di controllo a distanza dei lavoratori di cui all'articolo 4 della l. n. 300/1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dall'ambito di applicazione della norma i controlli diretti ad accertare condotte illecite del lavoratore (cd. controlli difensivi)" (cfr. Cass. n. 4746/2002), quali quelli messi in atto nel caso di specie;
l'utilizzo privato dell'elaboratore aziendale costituisce illecito contrattuale a carico del lavoratore; pertanto, la società poteva porre lecitamente in essere i necessari controlli difensivi volti a far valere i propri diritti.

§ 4 La decisione del Garante.

Il Garante ha accolto il ricorso del lavoratore. Dopo aver affrontato alcune questioni preliminari e formali circa l'irricevibilità del ricorso contestata dall'azienda (istanza respinta) l'Autorità ha affrontato le questioni di merito, che possono essere riassunte come segue:

l'azienda, 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;
l'azienda ha violato l'articolo 11 del Codice della privacy 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. In questa ottica, infatti, il Garante ha rilevato che dalla documentazione 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, 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;
proprio il fatto che il lavoratore - come dichiarato dall'azienda - non aveva necessità di accedere ad Internet per svolgere le proprie prestazioni, l'azienda avrebbe comunque potuto dimostrare l'illiceità del suo comportamento in rapporto al corretto uso degli strumenti affidati sul luogo di lavoro limitandosi a provare in altro modo la mera 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 (articolo 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" (articolo 26, comma 4, lett. c), del Codice; autorizzazione n. 1/2004 del Garante). Nel caso in questione il Garante non ha ritenuto sussistente il requisito della indispensabilità;
il trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale sarebbe stato 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, circostanza che il Garante non ha ritenuto sussistere nel caso in questione, nel quale sono stati fatti valere solo diritti legati allo svolgimento del rapporto di lavoro (cfr. articolo 26, comma 4, lett. c), del Codice; punto 3, lett. d), della citata autorizzazione; cfr. Provv. Garante 9 luglio 2003).

In considerazione di tutto quanto precede, l'Autorità ha dunque accolto il ricorso disponendo il blocco del trattamento e la inutilizzabilità dei relativi dati personali del lavoratore.

§ 5 Alcune considerazioni e riflessioni sulla decisione del Garante.

La decisione del Garante va correttamente inquadrata alla luce del quadro legale di riferimento, e ne va sicuramente chiarita la reale portata, anche in considerazione del fatto che le modalità con le quali la decisione è stata riportata dagli organi di stampa appaiono attribuire erroneamente al Garante l'affermazione di un principio assoluto e generale per il quale il controllo della navigazione effettuata dai lavoratori in Internet sarebbe sempre vietata.

Non è così. In primo luogo occorre chiarire la tipologia di atto: trattasi difatti di una decisione su un particolare ricorso e non di un provvedimento generale. In tale ottica, i principi richiamati dal Garante nelle motivazioni di accoglimento del ricorso, sono sì generali (principio di non eccedenza nei trattamenti, obbligo di preventiva informativa, principio del "pari rango" esimente del consenso nel caso di trattamento di dati idonei a rivelare lo stato di salute, etc), ma vengono applicati ad un caso specifico in cui l'Autorità ha rilevato - in modo del tutto corretto - il mancato rispetto del Codice della privacy. In termini più chiari, il Garante - in un peculiare caso portato alla sua attenzione del ricorso del lavoratore - ha dichiarato l'illiceità dei controllo sulla navigazione Internet del lavoratore non in via generale, ma a causa delle specifiche modalità con le quali tali controlli sono stati effettuati dall'azienda soccombente.
In secondo luogo, occorre ricordare che sulla tematica del controllo circa l'utilizzo da parte dei lavoratori di asset aziendali (quali Internet, email, software, apparati telefonici, etc) loro conferiti per l'esclusivo svolgimento delle mansioni lavoristiche (tematica sia privacy che lavoristica), la posizione della giurisprudenza (sia di merito che di Cassazione) è da molti anni assolutamente divergente da quanto a più riprese chiarito su tali temi dal Garante. In tal senso la decisione dell'Autorità sul caso specifico sopra analizzato è assolutamente in linea - e dunque non deve sorprendere - con la posizione che l'Autorità da sempre ha assunto. La problematicità della questione risiede difatti nella differente applicazione pratica dei (lacunosi) principi normativi esistenti, se è vero che la giurisprudenza di merito e di legittimità tende a riconoscere - a discapito della riservatezza dei lavoratori - la liceità dei poteri di controllo del datore di lavoro (a tutela della proprietà in capo allo stesso degli strumenti messi a disposizione del lavoratore per uso esclusivamente connesso allo svolgimento delle relative mansioni), mentre la giurisprudenza costituzionale ed i numerosi provvedimenti in materia sia del Garante che di altre autorità di settore (vedi ad esempio le indicazioni in merito del Gruppo dei Garanti europei) privilegiano in maniera netta la tutela della privacy dei lavoratori sul luogo di lavoro, anche rispetto all'utilizzo di risorse che dovrebbero essere destinate ad un uso esclusivamente lavorativo. Sul punto, si noti a margine che, a parere dello scrivente, l'argomento utilizzato dal lavoratore (dalla motivazione delle sentenze citate dall'azienda a sostegno delle proprie tesi difensive risulta che nei casi affrontati il controllo dei lavoratori è stato considerato lecito in quanto il trattamento di dati personali sarebbe stato breve e non eccedente, ovvero effettuato limitatamente ai tempi di connessione e non ai contenuti) e pure avallato dal Garante alla luce del principio di

"proporzionalità e non eccedenza" dei trattamenti non fotografa affatto l'attuale posizione della giurisprudenza, che in recenti sentenze - in divergenza con il Garante - afferma un potere di controllo datoriale ben più ampio che non è legato - nelle decisioni cui ci si riferisce - al requisito della "breve durata".
Bisogna altresì evidenziare che la tematica del controllo circa l'utilizzo da parte dei lavoratori di asset aziendali (quali Internet, email, software, apparati telefonici, etc) sconta l'assenza di chiare e specifiche regole (di rango normativo o deontologico), in quanto l'unico quadro legale cui ci si riferisce in casi analoghi è quello di cui all'articolo 4 dello Statuto dei Lavoratori (l. 20.5.1970, n. 300) necessariamente applicato analogicamente anche a mezzi - quali le nuove tecnologie intese come nuovi strumenti di assolvimento delle mansioni lavorative - non prevedibili neanche lontanamente all'epoca della redazione delle norme della l. 300/70. Sul punto è dunque ancora più grave la perdurante assenza del codice di deontologia e buona condotta sul trattamento dei dati personali nel settore del Lavoro e della Previdenza Sociale: si tratta di uno dei codici previsti dal d.lgs. 30.6.2003, n. 196 (Codice della privacy) che rinvia all'autoregolamentazione ed alla concertazione tra le parti interessate (nel caso: Confindustria e Organizzazioni Sindacali) la disciplina specifica del trattamento dei dati personali in particolari settori (sono già vigenti il codice deontologico sul trattamento dei dati personali in ambito giornalistico, in ambito statistico, storico e scientifico, nell'ambito dei sistemi informativi creditizi -centrali-rischi - private). Tale codice - che dovrebbe finalmente dettare norme specifiche anche sulle tematiche del controllo circa l'utilizzo da parte dei lavoratori di asset aziendali (quali Internet, email, software, apparati telefonici, etc) - è atteso dal 2004 e la sua mancata adozione determina necessariamente che questioni delicate quali quella in esame siano lasciate alla mera interpretazione giuridica e giurisprudenziale di un quadro normativo inadatto e lacunoso da parte dei competenti organi, con l'aggravante menzionata che le posizioni (del Garante e della Giurisprudenza) sono da tempo divergenti.
Effettuate le considerazioni di carattere generale che precedono, si procederà nel prosieguo all'analisi specifica di alcuni aspetti della decisione del Garante, anche alla luce delle argomentazioni svolte dall'azienda e dal lavoratore.
Riprendiamo dunque alcune tesi del lavoratore ricorrente ed analizziamole in rapporto alle effettive mancanze dell'azienda che hanno correttamente portato il Garante ad accogliere le contestazioni del lavoratore. Quest'ultimo afferma tra l'altro che l'azienda avrebbe trattato i 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'articolo 4 dello Statuto dei lavoratori che prevede che tale attività può avvenire solo previo consenso del sindacato o dell'ispettorato del lavoro. L'argomentazione è fondata. Ben avrebbe potuto (anzi: opportunamente dovuto) l'azienda - anche per contrastare validamente la contestazione avanzata dal dipendente - assolvere all'obbligo di preventiva informativa attraverso la redazione di un "regolamento interno sull'utilizzo delle risorse informatiche aziendali"(Internet, email, PC, software, apparati telefonici). Prima di proseguire lo svolgimento delle considerazioni sul punto, va osservato - anche come consiglio pratico alle imprese volto a prevenire contestazioni analoghe - che ogniqualvolta ciò risulti possibile la prevenzione dovrebbe essere considerata più importante del controllo. In altre parole l'interesse del datore di lavoro risulta servito meglio da una spesa destinata a prevenire gli abusi dell'Internet con mezzi tecnici piuttosto che ad individuare casi d'abuso. Se ed in quanto ragionevolmente possibile, la politica perseguita in rapporto all'Internet dovrebbe fare affidamento su mezzi tecnici per ridurre o filtrare l'accesso piuttosto che sul controllo dei comportamenti, basandosi ad esempio sul blocco di alcuni siti o sull'installazione di avvertenze automatiche per le richieste d'accesso a determinati siti. Ove ciò non risulti possibile, l'adozione del citato regolamento interno - adottato con i contenuti e le procedure che seguono - rappresenta allo stato la principale garanzia per il datore di lavoro (in vista della legittimità dei controlli), anche per quanto riguarda l'assolvimento degli obblighi di informativa privacy.
Il regolamento interno sull'utilizzo dei sistemi informatici dovrebbe disciplinare, in materia di utilizzo della connessione Internet (non si affrontano in questa sede gli altri profili relativi all'utilizzo di email, software, apparati telefonici, che pure implicano analoghe e delicate

questioni, laddove soggetti a controllo)- almeno i seguenti aspetti:
il datore di lavoro deve indicare chiaramente ai dipendenti che l'utilizzo di connessioni ad Internet deve essere destinato esclusivamente a finalità lavorative, indicando poi a quali condizioni è consentito l'impiego privato dell'Internet e precisando quale materiale non può essere visionato o copiato e spiegando ai dipendenti queste condizioni e questi limiti;
spiegazione del sistema di navigazione in essere, delle tecnologie di controllo (black list, firewall, etc.) delle finalità del controllo e della tipologia dei controlli attivati dall'azienda (inclusa la menzione della possibilità che talune informazioni sui lavoratori al di là di procedure di controllo - possono essere acquisite anche in occasione - ad esempio - della effettuazione di attività manutentive o di interventi tecnici)
i dipendenti vanno informati circa eventuali sistemi messi in opera per impedire l'accesso a determinati siti e per individuare i casi d'abuso. La portata di tali controlli andrà indicata, precisando ad esempio se essi possono riguardare singole persone o particolari sezioni dell'impresa oppure se in circostanze particolari il contenuto dei siti visitati è visionato o registrato dal datore di lavoro. La politica aziendale dovrà inoltre precisare quale uso può all'occorrenza venir fatto dei dati raccolti in rapporto alle persone che hanno visitato determinati siti;
i dipendenti vanno informati circa l'eventuale ripartizione dei costi di utilizzo delle connessioni al web;
i dipendenti vanno informati circa l'individuazione delle persone preposte al controllo (es: l'amministratore di rete quale responsabile del trattamento) e delle procedure in caso di eventuali azioni disciplinari;
i dipendenti vanno informati circa la partecipazione dei loro rappresentanti all'attuazione di tale politica e all'indagine sulle presunte infrazioni.
Ma soprattutto, oltre ai contenuti sopra riportati a titolo esemplificativo, l'aspetto dirimente della questione è rappresentato dalla procedura di adozione e concertazione del regolamento interno che deve necessariamente coinvolgere il lavoratore o le sue rappresentanze sindacali ai fini di quanto previsto dallo Statuto dei Lavoratori, e ciò anche per rendere successivamente legittimi controlli e susseguenti contestazioni disciplinari per violazione di regole interne concertate preventivamente con le organizzazioni sindacali. Da questo punto di vista una possibile procedura per l'adozione del regolamento aziendale sull'utilizzo delle risorse e dei sistemi informatici, dovrebbe prevedere le seguenti fasi:
stesura di una prima bozza del regolamento;
verifica da parte delle figure preposte;
eventuali modifiche;
stesura testo definitivo;
approvazione del testo dal parte del vertice aziendale;
incontro azienda-sindacato;
analisi del documento;
eventuali richieste di modifica o integrazioni da parte del sindacato;
modifiche al testo;
approvazione del testo modificato;
accordo tra sindacato e azienda;
diffusione della policy aziendale all'interno dell'azienda;
corsi di formazione per i lavoratori;
periodiche revisioni e aggiornamenti del documento.
Tutto ciò - per tornare al caso specifico in esame - non è stato realizzato dall'azienda, la quale si è richiamata genericamente al manuale della qualità che pur prevedendo apposite istruzioni per i lavoratori circa l'utilizzo delle risorse aziendali, non è parso - dalla ricostruzione della vicenda - né adeguatamente pubblicizzato all'interno della società (la mera esistenza dell'icona sul desktop è insufficiente ai fini di una corretta informativa), né - soprattutto - concertato preventivamente con i lavoratori e con le organizzazioni sindacali. Da questo punto di vista la contestazione del lavoratore e la successiva posizione del Garante sulla violazione degli obblighi di informativa appaiono del tutto fondate. E assolutamente inconcludente appare l'argomentazione difensiva

dell'azienda in base alla quale il lavoratore non era stato preventivamente informato di possibili controlli informatici in considerazione del fatto che gli accessi ad Internet, in virtù delle mansioni affidate al lavoratore, non sarebbero dovuti avvenire. Il caso deve dunque - sul punto - richiamare l'attenzione delle aziende sull'importanza dell'adozione del regolamento interno (laddove non si vogliano o non si possano adottare soluzioni tecniche diverse, quali il blocco o il filtraggio dei siti Internet), in base ai contenuti ed alle procedure di adozione sopra richiamate.
Il lavoratore contesta poi che il controllo sarebbe avvenuto non tanto sulla navigazione in Internet, quanto su proprie cartelle private appositamente create dallo stesso per salvare contenuti tratti dal web (il dipendente contesta infatti che l'azienda non ha trattato file di backup poiché dalla stringa contenuta nelle pagine sui dati sulle navigazioni riferite al lavoratore emerge che c'è stata un'operazione manuale di copia della "directory temporary internet files" contenuta in una apposita cartella, e analoga operazione sarebbe stata effettuata sulla cronologia delle navigazioni, non riferibile ad un backup automatico). Formalmente, la contestata violazione della riservatezza del lavoratore connessa alla citata condotta dell'azienda, appare fondata. L'azienda ha cioè controllato a distanza il lavoratore e non ha effettuato un controllo difensivo volto ad accertare l'illiceità dell'utilizzo dello strumento Internet dotazione ai dipendenti dell'azienda (e tra l'altro, il lavoratore in questione non era neanche abilitato alle connessioni web). Sul punto, sarebbe stato sufficiente prevedere nel regolamento interno sull'utilizzo delle risorse informatiche sopra riferito (ed ovviamente adottato con i contenuti e con le procedure di concertazione previste) il divieto per i lavoratori di creare autonomamente e senza autorizzazione del superiore gerarchico cartelle elettroniche estranee allo svolgimento delle mansioni lavorative. Se l'azienda avesse proceduto in tal modo, avrebbe potuto contestare - a parere dello scrivente - la violazione delle norme del codice civile, che si passa ad esaminare, che disciplinano il potere del datore di lavoro, nell'esercizio del proprio potere direttivo, di effettuare conseguenti controlli su come l'attività lavorativa viene svolta dal lavoratore (dipendente). L'articolo 2104 Cc dispone che il prestatore di lavoro deve usare la diligenza richiesta (1) dalla natura della prestazione dovuta, (2) dall'interesse dell'impresa (3) e dal quello superiore della produzione nazionale. Inoltre, egli deve osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartitegli dal datore o dai collaboratori di questi da cui il lavoratore gerarchicamente dipenda. L'articolo 2104 Cc pone dunque in capo al lavoratore il cosiddetto "obbligo di diligenza". Il successivo articolo 2105 Cc disciplina invece un obbligo di natura diversa: quello di fedeltà al datore di lavoro, disponendo che il lavoratore non può trattare affari, in proprio o per conto terzi, in concorrenza con il datore di lavoro (definito dal codice "imprenditore"), né divulgare notizie attinenti all'organizzazione e ai metodi di produzione dell'impresa, o farne uso in modo da potere recare ad essa pregiudizio. Anche se il cosiddetto "obbligo di fedeltà" è qualificato precisamente dalla norma (quale divieto di non porre in essere condotte anticoncorrenziali, o lesive della riservatezza a tutela del patrimonio informativo aziendale), il riferimento generico al divieto di condotte che possano recare pregiudizio all'impresa può essere letto (e la giurisprudenza ne dà questa lettura) nel senso di imporre al lavoratore un obbligo di fedeltà che deve permeare in generale tutto lo svolgimento dell'attività lavorativa.
Dal momento che il successivo articolo 2106 Cc prevede l'applicazione di sanzioni disciplinari (graduate secondo il tipico sistema lavoristico in base alla gravità dell'infrazione, dunque dal semplice richiamo fino alla sanzione più grave del licenziamento) in capo al lavoratore che abbia violato i suoi doveri di diligenza e fedeltà, ne parrebbe discendere che i poteri di controllo del datore di lavoro altro non sono se non uno dei più efficaci strumenti per verificare (anche dal punto di vista contrattuale) l'esatto adempimento della prestazione lavorativa dei suoi dipendenti, per di più alla luce dei principi codicistici appena menzionati. Il problema diventa allora quello di individuare i limiti di tali poteri datoriali, che diventano legittimi solo se contemperati con l'altrettanta fondamentale esigenza di garantire la riservatezza, la libertà e la dignità dei lavoratori. In sostanza, il punto è quello di individuare i limiti di "invasività" della privacy del lavoratore consentita al datore che intenda verificare la diligenza, la fedeltà e l'esatto adempimento della prestazione lavorativa, sul presupposto - comunque generalmente riconosciuto - che per tali finalità il lavoratore deve comunque consapevolmente subire - sul posto di lavoro - una intrusione (purchè tollerabile) della propria sfera personale.

Si intende dire che se l'azienda in questione avesse adottato il regolamento interno sull'utilizzo delle risorse informatiche (lo si ripete: con i contenuti e le procedure concertate sopra riferite) tale regolamento avrebbe potuto valere quale insieme di "disposizioni per l'esecuzione e per la disciplina del lavoro impartitegli dal datore o dai collaboratori di questi da cui il lavoratore gerarchicamente dipenda" (articolo 2104 Cc) che il lavoratore sarebbe stato tenuto ad osservare. In sostanza, se questa fosse stata la situazione, e se il divieto di creare autonomamente cartelle per la conservazione di materiali estranei alle mansioni lavorative fosse stato specificatamente previsto nel regolamento interno, l'azienda si sarebbe potuta trovare nella opposta situazione di contestare la violazione dell'articolo 2104 Cc, invece di soccombere proprio sulla contestazione di aver violato la privacy consultando a distanza le directories del dipendente. E probabilmente, ciò avrebbe anche potuto superare la fondata considerazione del Garante circa il fatto che l'azienda ha proceduto ad un trattamento eccedente e non proporzionato (relativo al controllo della cartella contenente i materiali salvati dal web) perchè che il lavoratore non aveva l'abilitazione ad accedere ad Internet e sarebbe stato sufficiente dimostrare la mera connessione al web (non rientrante negli strumenti in dotazione a quel lavoratore) prescindendo dal dettaglio dei contenuti dei siti visitati e dei dati sensibili trattati.
Altra e diversa considerazione attiene alla fondata contestazione del lavoratore circa il fatto che l'unica password da lui utilizzata era la "password utente" che consente di avviare la sessione di lavoro sul computer, mentre nessuna password era prevista per entrare nella rete Internet, liberamente accessibile mediante l'icona relativa al browser Explorer di Windows. Ancora una volta, sarebbe stato opportuno che l'azienda adottasse preventive (e semplici) procedure gestionali del mansionario del lavoratore per ovviare alla relativa contestazione (o almeno depotenziarne la portata in sede di contestazione). Se infatti l'azienda avesse dotato i lavoratori autorizzati (in base alle relative mansioni) ad accedere a Internet di specifiche credenziali di autenticazione specificatamente abilitanti all'accesso al web, probabilmente la questione non si sarebbe neanche posta. Ciò testimonia l'importanza (alla quale spesso corrisponde una colpevole - e dannosa, come dimostra il caso in questione - disattenzione nell'organizzazione delle imprese) della adozione di scelte gestionali assolutamente non onerose e tecnicamente facilmente attuabili (filtraggio o blocco della possibilità di visitare certi siti Internet unitamente alla abilitazione alla navigazione web dei soli dipendenti che ne abbiano la necessità per l'esclusivo svolgimento delle mansioni loro affidate).
Concludendo la rassegna di alcune delle considerazioni che il caso analizzato solleva, non si può non concordare pienamente con la violazione del cosiddetto "principio del pari rango" che il Garante ha contestato all'azienda circa il trattamento dei dati sensibili e idonei a rivelare le abitudini sessuali dell'interessato implicato dagli esiti dei controlli sui siti pornografici visitati dal dipendente. Nel rinviare alle considerazioni autoesplicative svolte dall'Autorità (ed alle norme ed autorizzazioni dalla stessa richiamate), va ricordato che fin dal 2003 il Garante, con provvedimento del 9 Luglio, ha chiarito cosa si intende per "pari rango". In tale provvedimento, l'Autorità ha precisato che il trattamento da parte di un terzo dei dati idonei a rivelare lo stato di salute o le abitudini sessuali è legittimo (in assenza della preventiva richiesta di consenso scritto all'interessato) solo se i diritti da far valere attraverso tale trattamento da colui che tratta le relative informazioni sono di "pari rango". In tale ottica occorre avere presente, quale elemento di raffronto per il bilanciamento degli interessi (cioè dei diritti di colui che tratta le informazioni e del diritto alla riservatezza dell'interessato cui i dati si riferiscono), non già il diritto alla tutela giurisdizionale, che pure è costituzionalmente garantito, bensì il diritto soggettivo sottostante, che si intende far valere sulla base dei dati oggetto di trattamento di cui si vorrebbe avere conoscenza. Il trattamento di dati che rientrano nella sfera di riservatezza dell'interessato può ritenersi giustificato e legittimo solo se il diritto del soggetto che li tratta rientra nella categoria dei diritti della personalità (i diritti della personalità, conosciuti anche come diritti personalissimi, sono quelli riconosciuti a una persona indipendentemente dal fatto di trovarsi in relazione con altre persone o cose: vi rientrano per esempio il diritto al nome, all'immagine, all'integrità fisica. Si tratta di diritti assoluti, ossia di diritti che possono essere fatti valere nei confronti di chiunque dovesse contestarne l'esercizio, e intrasmissibili: il titolare, cioè, non può trasferirli ad altri) o è compreso tra altri diritti fondamentali ed inviolabili (es: quelli garantiti dalla Costituzione, libertà

personale, inviolabilità del domicilio, libertà di manifestazione del pensiero, etc). Alla luce di tali principi - sinteticamente richiamati - che il Garante ha chiarito fin dal 2003 e la cui applicazione al caso esaminato non è altro che una coerente conseguenza della posizione dell'Autorità, appare evidente che il trattamento di dati idonei a rivelare lo stato di salute e la vita sessuale del lavoratore (implicato dalla scoperta dei siti Internet a contenuto pornografico) sarebbe stato lecito solo per far valere o difendere in giudizio un diritto di rango pari a quello del lavoratore, circostanza che il Garante non ha ritenuto sussistere nel caso in questione, nel quale sono stati fatti valere solo diritti legati allo svolgimento del rapporto di lavoro.

§ 6 Conclusioni.
L'analisi del caso che ha visto opposti il lavoratore e l'azienda, e le conseguenti valutazioni che più sopra sono state riferite, dovrebbe dunque portare a confermare la corretta portata della decisione del Garante, la quale - come si diceva all'inizio - non ha di certo introdotto un principio generale di divieto assoluto per il datore di lavoro di controllare la navigazione su Internet da parte dei propri dipendenti sul posto di lavoro (e con risorse aziendali).

Inoltre, occorre altresì ricordare che l'Autorità - come essa stessa afferma nel suo provvedimento decisorio ("la presente decisione lascia impregiudicati i diritti delle parti in ordine alla liceità o meno dei comportamenti addebitati al ricorrente") - ha affrontato i profili della questione con limitato riferimento alla sua competenza amministrativa (in sede di decisioni su ricorsi) a valutare la conformità dei fatti al vigente quadro normativo in materia di tutela dei dati personali. In sostanza, altre importanti questioni che pure rilevano sul piano lavoristico o penale (il lavoratore ha effettuato accessi non a PC aziendali; il lavoratore si è appropriato del materiale cartaceo utilizzato per stampare i risultati della navigazione; il lavoratore ha danneggiato la rete aziendale a causa dei virus informatici introdottisi a seguito della navigazione non consentita nei siti Internet contestati) sono ovviamente demandate alla competenza delle autorità giurisdizionali. E' dunque probabile attendersi ulteriori sviluppi della questione, sia con riferimento ai citati e diversi profili di competenza giurisdizionale che il Garante non poteva ovviamente affrontare, sia con riferimento alle stesse conclusioni che l'Autorità - in accoglimento del ricorso del lavoratore - ha evidenziato nella sua decisione. Ai sensi dell'articolo 151 del Codice della privacy, infatti, avverso il provvedimento espresso o il rigetto tacito con cui il Garante definisce un ricorso presentato, il titolare o l'interessato possono proporre opposizione con ricorso all'autorità giudiziaria, in base ad una particolare e innovativa procedura prevista dal successivo articolo 152. Potrebbe dunque essere possibile che la sopra menzionata divergenza tra le posizioni assunte dalla recente giurisprudenza e quelle espresse dal Garante in materia di controllo circa la navigazione Internet e l'uso della posta elettronica sul luogo di lavoro portino i giudici a ribaltare la decisione amministrativa ad oggi favorevole al lavoratore.
*Avvocato, Studio legale Tonucci, responsabile del Dipartimento Data Protection