# Ordine dei Dottori Commercialisti e degli Esperti Contabili di Brescia

Commissione organizzazione dello studio e informatica

## VADEMECUM N.1

DISCIPLINARE INTERNO
SULL'USO DELLA POSTA ELETTRONICA E DI INTERNET

Commissione Organizzazione dello studio e informatica:Rag. Gianantonio Poli (coordinatore), Rag. Elisabetta Migliorati (cons. delegato dell'Ordine), Dott. Maurizio Bacchiega, Rag. Aldo Bertana, Dott.ssa Francesca Bertelli, Dott. Luca Calzolari, Dott. Davide Felappi, Dott. Rag. Filippo Fornari, Dott. Stefano Guerrini, Dott. Biagio Notario, Dott. Aldo Massimo Rossi, Rag. Eugenia Salvadori, Dott. Marco Scardeoni, Dott. Paolo Tebaldini, Rag. Carlo Valetti, Dott. Fabio Zotti.

# DISCIPLINARE INTERNO
# SULL'USO DELLA POSTA ELETTRONICA E DI INTERNET
# (FAC SIMILE)

PREMESSO

- che con il Provvedimento del 1.03.2007 pubblicato sulla Gazzetta Ufficiale del 10.03.2007, n. 58, dal titolo *"Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori"* (1) il Garante per la protezione dei dati personali raccomanda l'adozione da parte dei datori di lavoro pubblici e privati, di un "Disciplinare interno" (punto 3.2) in cui siano indicate le regole per l'uso di sistemi informatici da parte del personale dipendente;

- che compete allo studio assicurare la disponibilità, l'integrità ed il corretto funzionamento dei sistemi informatici in dotazione al personale dipendente durante il rapporto di lavoro e adottare idonee misure di sicurezza per prevenire indebiti utilizzi che possano essere fonte di responsabilità nel rispetto del Decreto Legislativo 30.06.2003, n. 196 (Codice in materia di protezione dei dati personali) e succ. mod.

- che compete allo studio tutelare, nel rispetto reciproco di diritti e doveri, le informazioni di carattere personale trattate che possono riguardare, oltre l'attività lavorativa, la sfera personale e la vita privata dei dipendenti dello studio nel rispetto della Legge 20.05.1970, n. 300 ( Statuto dei lavoratori ).

TUTTO CIO' PREMESSO

lo studio adotta il seguente Disciplinare Interno rivolto al personale dipendente.

## 1. ADOZIONE DI MISURE DI TIPO ORGANIZZATIVO

### 1.1 Valutazione dell'impatto sui diritti del personale di studio

Lo studio professionale , quale luogo di lavoro, è una formazione sociale e in quanto tale va preservata assicurando la tutela dei diritti, delle libertà fondamentali e della dignità del personale garantendo l'esplicazione della singola personalità e la ragionevole protezione della sua sfera di riservatezza nelle relazioni personali. Il personale dipendente è tenuto a sua volta ad adeguarsi alle disposizioni qui contenute, evitando, durante il rapporto di lavoro, utilizzi indebiti dei sistemi informatici in dotazione che possano arrecare disturbo o danno allo studio ;

### 1.2 Tipologie di sistemi informatici e personale dipendente autorizzato

Per utilizzo dei sistemi informatici dello studio si intende :
- l'accesso e navigazione in internet ;
- l'utilizzo della posta elettronica ;
- la tenuta dello spazio di memorizzazione (hard disk) in dotazione.

Al personale autorizzato all'utilizzo della navigazione in internet e all'utilizzo della casella di posta elettronica vengono assegnate le postazioni di lavoro contrassegnate sulla pianta dei locali di studio qui allegata.

### 1.3 Ubicazione postazioni di lavoro

Lo studio si riserva di prefigurare le modalità d'uso della navigazione in internet e della posta elettronica nei luoghi e nei tempi così definiti : utilizzo dei sistemi informatici a fini di lavoro durante il normale orario di studio. E' consentito l'uso moderato dei medesimi per finalità private nei momenti di pausa o fuori dall'orario di lavoro nelle aree di lavoro riservate. Lo studio può in qualsiasi momento autorizzare in caso di sopravvenuta urgente necessità o forza maggiore l'uso privato delle postazioni di lavoro assegnate.

(1) Il testo del Provvedimento del 1.03.2007 pubblicato sulla Gazzetta Ufficiale del 10.03.2007, n. 58 del Garante per la Privacy è riprodotto in allegato - fonte http://www.cnipa.gov.it

## 2. ADOZIONE DI MISURE DI TIPO TECNOLOGICO

### 2.1 Accesso e navigazione in internet ed uso dei sistemi informatici

L'uso di internet nelle sue numerose funzionalità è consentito esclusivamente per gli scopi attinenti al proprio lavoro svolto presso la sede o le sedi dello studio professionale.

Lo studio non ha definito un elenco di siti internet autorizzati, tuttavia è permesso l'utilizzo di appositi strumenti di filtraggio, mediante i quali può essere bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come estranei agli interessi ed alle attività dello studio professionale. II divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video.

Non è permessa la possibilità di scaricare (download) da internet file musicali, video o software che non siano necessari alla propria attività di studio, salvo l'ascolto di web- radio previo assenso del titolare di studio a seconda delle zone di lavoro e previo controllo attivo da parte di software anti-intrusione.

E' vietato l'utilizzo delle risorse dei sistemi informatici di studio per la memorizzazione di materiale digitale privato, personale o non attinente all'attività lavorativa.

Relativamente all'utilizzo dei singoli sistemi informatici di studio relativi alla postazione di lavoro si precisa che l'assegnazione della risorsa non ne comporta la privatezza, in quanto trattasi di strumento di esclusiva proprietà dello studio, e quindi i files memorizzati non sono né tutelati né garantiti dallo studio per qualsiasi causa.

### 2.2 Uso della posta elettronica

Lo studio assegna indirizzi di posta elettronica per ogni posto di lavoro. Al singolo dipendente può essere assegnato un indirizzo e-mail personale e/o anche generale di segreteria di studio.
La "personalizzazione" dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di esclusiva proprietà dello studio, messi a disposizione del dipendente o collaboratore al solo fine dello svolgimento delle proprie mansioni lavorative.

I messaggi inviati tramite posta elettronica dello studio (generale e/o nominativa) potranno riportare in aggiunta il seguente testo: "*Il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal disciplinare di studio adottato in materia.*

E' ammesso l'utilizzo di sistemi di web-mail personali e private con modalità e tempi tali da non incidere negativamente sull'attività di lavoro come stabilito al punto 1.3.

### 2.3 Memorizzazione files log di navigazione in internet

Al fine di verificare la funzionalità, la sicurezza del sistema di navigazione internet all'interno dello studio ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet e al traffico della casella di posta elettronica, memorizzano un giornale (file di log) contenente le informazioni relative ai siti che i sistemi informatici di studio hanno visitato. Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'utente, garantendo in tal modo il suo anonimato. I sistemi software sono programmati e configurati in modo da cancellare mensilmente i dati relativi agli accessi ad Internet ed al traffico telematico.

L'accesso a questi dati è effettuato dal personale incaricato dalla ditta di manutenzione del software e hardware di studio ed eventualmente da altro personale tecnico esterno autorizzato.

L'eventuale prolungamento dei suddetti tempi di conservazione è eccezionale e può avere luogo solo in relazione all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

## 3. CONTROLLI

### 3.1 Controlli della navigazione internet e della posta elettronica

Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo, lo studio effettua con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi:

- analisi aggregata del traffico di rete riferito all'intera della struttura lavorativa di studio o a sue aree e rilevazione della tipologia di utilizzo (e-mail, file audio, accesso a risorse estranee alle mansioni);

- riscontro eventuale utilizzo anomalo dei sistemi informatici dello studio e affissione di avviso generalizzato, con l'invito ad attenersi scrupolosamente alle indicazioni del presente Disciplinare Interno ed alle istruzioni impartite. Eventuale richiamo all'osservanza delle regole può essere circoscritto agli operatori nella zona di studio in cui è stata rilevata l'anomalia;

- in caso di successivo permanere della situazione non conforme con reiterati utilizzi anomali, lo studio potrà effettuare controlli circoscritti su singole postazioni di lavoro.

### 3.2 Controlli dell'occupazione dello spazio di memorizzazione dei sistemi informatici

Qualora le misure tecniche preventive non fossero sufficienti ad evitare eventi dannosi o situazioni di pericolo riguardo l'occupazione dello spazio di memorizzazione (hard-disk), lo studio effettua con gradualità, nel rispetto dei principi di pertinenza e non eccedenza, le verifiche di eventuali situazioni anomale attraverso le seguenti fasi

- analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa di studio e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato ) e relativa pertinenza con l'attività lavorativa;

- emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumentali informatici di studio, con l'invito ad attenersi scrupolosamente ; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti la zona di studio in cui è stata rilevata l'anomalia;

- in caso di successivo permanere di una situazione non conforme, sarà possibile procedere con un analisi puntuale ed una eventuale eliminazione del materiale non conforme anche sulle singole postazioni di lavoro.

## 4. TELEASSISTENZA E TELELAVORO IN REMOTO

In caso di attività di manutenzione in remoto di hardware e software su personal computer singoli o connessi alla rete di studio, il personale della ditta di manutenzione e/o la società fornitrice dei gestionali di studio potranno utilizzare specifici software allo scopo.
Tali programmi vengono utilizzati per assistere l'utente durante la normale attività informatica o durante la manutenzione di applicativi e/o hardware di studio.
L'attività di assistenza e manutenzione, previa autorizzazione telefonica da parte dell'utente interessato, avviene per il tramite di un codice invito assegnato dalle ditte autorizzate.
Viene fornito manuale per le modalità del suo utilizzo per tutti i soggetti delle postazioni di lavoro interessate.

Le disposizione del presente disciplinare si applicano anche in caso di utilizzo di dispositivi mobili e/o notebook, messi a disposizione dallo studio, in caso di tele-lavoro in remoto.

## 5. CONTINUITA' LAVORATIVA IN CASO DI ASSENZA DEL DIPENDENTE

In caso di assenza di un dipendente dello studio, previa autorizzazione del Responsabile al trattamento dei dati, questi può, anche da postazioni esterne all'azienda, utilizzare specifiche funzionalità di posta elettronica tipo web-mail per inviare messaggi di risposta che informino il mittente della propria temporanea indisponibilità, e inoltrare messaggi ricevuti verso indirizzi di altro personale dipendente dello studio.

Nel caso il dipendente si assenti e non possa fare uso di dette funzionalità , il Responsabile del trattamento dei dati., potrà delegare un incaricato affinché acceda alla casella di posta elettronica al fine di garantire la continuità dell'attività lavorativa.

## 6. PROVVEDIMENTI DISCIPLINARI

Qualora il personale addetto incaricato dallo studio, durante i controlli di cui ai punti 3.1 e 3.2, anche riguardo al particolare utilizzo di cui al punto 4, rilevi anomalie nell'utilizzo dei sistemi informatici che possano essere configurate quali attività non conformi al presente disciplinare , provvederà ad informare il Responsabile del trattamento dei dati il quale, effettuate le verifiche del caso, segnalerà il fatto al Titolare del trattamento dei dati e titolare di studio per le valutazioni di competenza e per i procedimenti disciplinari del caso.

A seguito dell'accertamento della condotta illecita e, quindi, dell'adozione del provvedimento disciplinare, lo studio si riserva di segnalare l'abuso anche all'Autorità competente.

## 7. USO PERSONALE DI MEZZI INFORMATICI DI STUDIO A CARICO DELL'INTERESSATO

Non sono previste modalità di uso privato dei sistemi informatici dello studio con pagamento o fatturazione a carico del personale interessato.

## 8. INFORMATIVA AI SENSI DELL'ART. 13 D.LG.VO 196/03

Il Titolare del trattamento dei dati personali relativo all'utilizzo di strumenti informatici da parte dei dipendenti è lo studio nella persona del Sig. .
Il Responsabile del trattamento dei dati Sig. tramite personale tecnico interno incaricato al trattamento dei dati o personale tecnico esterno autorizzato effettueranno il trattamento dei dati con strumenti informatici. L'Incaricato al trattamento dei dati è il Sig. .
La finalità del trattamento è la verifica del corretto utilizzo della posta elettronica, della rete internet e degli spazi di memorizzazione (hard-disk) da parte dei dipendenti di studio nel rapporto di lavoro.
II trattamento di verifica è effettuato con modalità di gradualità e per aree aggregate per cui i dati non vengono comunicati con riferimento al trattamento del singolo dipendente; la comunicazione, nel caso in cui si accerti un uso indebito della singola postazione, sarà data al Responsabile del trattamento dei dati dello studio per la valutazione del caso sotto il profilo disciplinare.
II dipendente potrà far valere i diritti di cui all'art. 7 del D.Lgs 196/03 facendo pervenire richiesta scritta al Titolare e al Responsabile del trattamento dei dati.

## 9. MISURE DI SICUREZZA

Per quanto riguarda le misure di sicurezza dei dati e dei sistemi si rimanda al DPS (Documento Programmatico sulla Sicurezza) adottato dallo studio in data e aggiornato con cadenza annuale.

Il Responsabile del trattamento dei dati Il Titolare del trattamento dei dati

# Provvedimento 1° marzo 2007 del Garante per la protezione dei dati personali

# "Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori.".

G.U. 10 marzo 2007, n. 58

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- In data odierna, in presenza del prof. Francesco Pizzetti, presidente, del dott. Giuseppe Chiaravalloti, vice presidente, del dott. Giuseppe Fortunato e del dottor Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;
- Visti i reclami, le segnalazioni e i quesiti pervenuti riguardo ai trattamenti di dati personali effettuati da datori di lavoro riguardo all'uso, da parte di lavoratori, di strumenti informatici e telematici;
- Vista la documentazione in atti;
- Visti gli articoli 24 e 154, comma 1, lettere *b*) e *c*) del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196);
- Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;
- Relatore il dott. Mauro Paissan;

Premesso

## 1. Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro.

1.1. Premessa.

Dall'esame di diversi reclami, segnalazioni e quesiti è emersa l'esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.

Occorre muovere da alcune premesse:

a. compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;

b. spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità *(articoli 15, 31 ss., 167 e 169 del Codice)*;

c. emerge l'esigenza di tutelare i lavoratori interessati anche perchè l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;

d. l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di *log file* della navigazione *web* ottenuti, ad esempio, da un *proxy server* o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di *log file* di traffico *e-mail* e l'archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

e. le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

1.2. Tutela del lavoratore.

Le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi.

La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, può essere tracciata a volte solo con difficoltà.

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali *(articoli 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato).*

Non a caso, nell'organizzare l'attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

## 2. Codice in materia di protezione dei dati e discipline di settore.

2.1. Principi generali.

Nell'impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizzazione ed efficacia *(articoli 1 e 2 del Codice).* Le prescrizioni potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

2.2. Discipline di settore.

Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza *(articoli 113, 114 e 184, comma 3, del Codice; articoli 4 e 8 legge 20 maggio 1970, n. 300).*

La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente *(art. 47, comma 3, lettera b) Codice dell'amministrazione digitale*[)].

2.3. Principi del Codice.

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell'osservanza di alcuni cogenti principi:

a. il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite *(art. 3 del Codice; paragrafo 5.2)*;

b. il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori *(art. 11, comma 1, lettera a), del Codice).* Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati *(v. paragrafo 3)*;

c. i trattamenti devono essere effettuati per finalità *determinate, esplicite e legittime (art. 11, comma 1, lettera b), del Codice: paragrafi 4 e 5),* osservando il principio di pertinenza e non eccedenza *(par. 6).* Il datore di lavoro deve trattare i dati «nella misura meno invasiva possibile»; le attività di monitoraggio devono essere svolte solo da soggetti preposti *(par. 8)* ed essere *«mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza» (Parere n. 8/2001, cit., punti 5 e 12).*

## 3. Controlli e correttezza nel trattamento.

3.1. Disciplina interna.

In base al richiamato principio di correttezza, l'eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore *(art. 4, secondo comma, Statuto dei lavoratori; allegato VII, paragrafo 3 d.lg. n. 626/1994 e successive integrazioni e modificazioni in materia di «uso di attrezzature munite di videoterminali», il quale esclude la possibilità del controllo informatico «all'insaputa dei lavoratori».*

Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

3.2. Linee guida.

In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

A seconda dei casi andrebbe ad esempio specificato:

- se determinati comportamenti non sono tollerati rispetto alla «navigazione» in Internet (ad es., il *download* di *software* o di *file* musicali), oppure alla tenuta di *file* nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l'arco temporale di utilizzo (ad es., fuori dall'orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);
- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di *file* di *log* eventualmente registrati) e chi (anche all'esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime - specifiche e non generiche - per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso

(specie se programmata), con particolare riferimento all'attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;

- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell'interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l'eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi *(art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10).*

3.3. Informativa (art. 13 del Codice).

All'onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell'art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2.

Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.

Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando comportano un trattamento lecito di dati *(art. 4, secondo comma, legge n. 300/1970)*; possono anche riguardare l'esercizio di un diritto in sede giudiziaria.

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

## 4. Apparecchiature preordinate al controllo a distanza.

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime *(art. 11, comma 1, lettera b*), *del Codice)*, il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro *(cfr. articoli 2086, 2087 e 2104 cod. civ.)*.

Nell'esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare *«apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori» (art. 4, primo comma, legge n. 300/1970)*, tra cui sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell'utente di un sistema di comunicazione elettronica.

Il trattamento dei dati che ne consegue è illecito, a prescindere dall'illiceità dell'installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli.

In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire - a volte anche minuziosamente - l'attività di lavoratori. È il caso, ad esempio:

- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell'analisi occulta di *computer* portatili affidati in uso.

Il controllo a distanza vietato dalla legge riguarda l'attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro. A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili *(art. 11, comma 2, del Codice).*

## 5. Programmi che consentono controlli «indiretti».

5.1. Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori *(art. 4, comma 2)*, di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Ciò, anche in presenza di attività di controllo discontinue.

Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

5.2. Principio di necessità.

In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all'adozione di misure «repressive») e, comunque, a «minimizzare» l'uso di dati riferibili ai lavoratori *(articoli 3, 11, comma 1, lettera d) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4).*

Dal punto di vista *organizzativo* è quindi opportuno che:

- si valuti attentamente l'impatto sui diritti dei lavoratori (prima dell'installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell'eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e l'accesso a Internet;
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l'onere di adottare tutte le misure *tecnologiche* volte a minimizzare l'uso di dati identificativi (c.d. *privacy* enhancing technologie PETs). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad esempio, posta elettronica o navigazione in Internet):

a. *Internet: la navigazione web.* - Il datore di lavoro, per ridurre il rischio di usi impropri della «navigazione» in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'*upload* o il *download* di *file*, l'uso di servizi di rete con finalità ludiche o estranee all'attivita), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale *(art. 8 legge n. 300/1970; articoli 26 e 113 del Codice; Provv. 2 febbraio 2006, cit.).*

   In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:

   - individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
   - configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni - reputate inconferenti con l'attività lavorativa - quali l'*upload* o l'accesso a determinati siti (inseriti in una sorta di *black list*) e/o il *download* di *file* o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato);
   - trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad esempio, con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
   - eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza;

b. *Posta elettronica*. - Il contenuto dei messaggi di posta elettronica - come pure i dati esteriori delle comunicazioni e i *file* allegati - riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti *(articoli 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale).*

   Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell'organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una *policy* al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.

Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta «in entrata») o di quelli inviati da quest'ultimo (posta «in uscita»).

È quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull'eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami @società.com, urp@ente.it, ecc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi @ente.it, rossi@società.com, mario.rossi@società.it);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore,
- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad esempio, per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le «coordinate» (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. È parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. In caso di eventuali assenze non programmate (ad esempio, per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad esempio, l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell'organizzazione di

appartenenza del mittente e con eventuale rinvio alla predetta *policy* datoriale.

## 6. Pertinenza e non eccedenza.

6.1. Graduazione dei controlli.

Nell'effettuare controlli sull'uso degli strumenti elettronici deve essere evitata un'interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

L'eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

6.2. Conservazione.

I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei *log file*) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario - e predeterminato - a raggiungerla *(v. art. 11, comma 1, lettera e), del Codice)*.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali numeri 1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

## 7. Presupposti di liceità del trattamento: bilanciamento di interessi.

7.1. Datori di lavoro privati.

I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati *(v., in particolare, art. 4, secondo comma, dello Statuto)*, possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili.

Ciò, può avvenire:

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

c. in caso di valida manifestazione di un libero consenso;

d. anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi *(art. 24, comma 1, lettera g), del Codice)*.

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo «indiretto» a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l'autorizzazione di un organo periferico dell'amministrazione del lavoro).

L'eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26).

7.2. Datori di lavoro pubblici.

Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (articoli 18-22 e 112).

In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi *(art. 7, comma 4, lettera a), del Codice)*.

## 8. Individuazione dei soggetti preposti.

Il datore di lavoro può ritenere utile la designazione (facoltativa), specie in strutture articolate, di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità (art. 29 del Codice).

Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti.

Resta fermo l'obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.

Resta parimenti ferma la necessità che, nell'individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un'attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni *(cfr. allegato B) al Codice, regola n. 19.6; Parere n. 8/2001 cit., punto 9)*.

Tutto ciò premesso il Garante:

1. prescrive ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lettera *c*), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l'onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;
2. indica inoltre, ai medesimi datori di lavoro, le seguenti linee guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:
    a. l'adozione e la pubblicizzazione di un disciplinare interno (punto 3.2.);
    b. l'adozione di misure di tipo organizzativo (punto 5.2.) affinchè, segnatamente:
        - si proceda ad un'attenta valutazione dell'impatto sui diritti dei lavoratori;
        - si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l'utilizzo della posta elettronica e dell'accesso a Internet;
        - si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;
    c. l'adozione di misure di tipo tecnologico, e segnatamente:
        I. rispetto alla «navigazione» in Internet (punto 5.2., *a*):
            - l'individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
            - la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni;
            - il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione degli utenti mediante opportune aggregazioni;
            - l'eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
            - la graduazione dei controlli (punto 6.1.);
        II. rispetto all'utilizzo della posta elettronica (punto 5.2., *b*):

- la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
- l'eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
- la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le «coordinate» di altro soggetto o altre utili modalità di contatto dell'istituzione presso la quale opera il lavoratore assente;
- consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, l'interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- l'inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente;
- la graduazione dei controlli (punto 6.1.);

3. vieta ai datori di lavoro privati e pubblici, ai sensi dell'art. 154, comma 1, lettera *d*), del Codice, di effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al controllo a distanza di lavoratori (punto 4), svolti in particolare mediante:
    a. la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
    b. la riproduzione e l'eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
    c. la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
    d. l'analisi occulta di *computer* portatili affidati in uso;
4. individua, ai sensi dell'art. 24, comma 1, lettera *g*), del Codice, nei termini di cui in motivazione (punto 7), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati;
5. dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia - Ufficio pubblicazione leggi e decreti, per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.