MEF Dipartimento delle Finanze

Posta elettronica

Direttive per l'utilizzo

Sommario

Direttive sull'utilizzo della posta nella P.A.

Direttiva del 27 novembre 2003 (Direttiva per l'impiego della posta elettronica nelle pubbliche amministrazioni)

IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE

EMANA LA SEGUENTE DIRETTIVA PER L'IMPIEGO DELLA POSTA ELETTRONICA NELLE PUBBLICHE AMMINISTRAZIONI

PARAGRAFO I

Il Consiglio dei Ministri, in data 31 maggio 2002, ha approvato le "Linee guida per lo sviluppo della società dell'informazione nella legislatura" nelle quali è contenuto l'obiettivo di adottare, entro la fine della legislatura, la posta elettronica per tutte le comunicazioni interne alla Pubblica Amministrazione.

L'impiego della posta elettronica consente e facilita quel cambiamento culturale ed organizzativo della Pubblica Amministrazione che risponde alle attese del Paese ed alle sfide della competitività: bisogna accelerare questo processo di cambiamento e darne concreta percezione anche all'esterno, abbandonando inutili ed onerosi formalismi, considerati, anche, i consistenti risparmi di risorse che potranno derivare alla Pubblica Amministrazione dall'uso intensivo della posta elettronica. Bisogna concretamente operare affinché di tale cambiamento possano beneficiare, al più presto, anche i cittadini e le imprese in modo da consentire loro un accesso più veloce e più agevole alle Pubbliche Amministrazioni.

In tale ottica, nell'esercizio della delega attribuita dal Parlamento al Governo con la legge 29 luglio 2003, n. 229, si intende, inoltre, accelerare ulteriormente il processo di trasparenza. A tal fine la completa attuazione del protocollo informatico (il cui avvio è previsto per il primo gennaio del 2004) consentirà la gestione dei flussi dei procedimenti in corso presso le pubbliche Amministrazioni permettendo di conoscerne lo stato e realizzando, così, un più elevato livello di trasparenza dell'azione amministrativa.

Nell'esercizio della suddetta delega saranno anche fissati i tempi di attuazione dell'intero nuovo processo che deve tener conto della necessità di operare il cambiamento in tempi rapidi**,** per evitare la coesistenza prolungata delle procedure elettroniche con quelle tradizionali**,** allo scopo di superare difficoltà organizzative e gestionali e ridurre i relativi costi operativi.

Il Comitato dei Ministri per la Società dell'Informazione, nel ribadire l'importanza di tali obiettivi, in data 18 marzo 2003, ha approvato un progetto di sostegno alla diffusione della posta elettronica nelle Amministrazioni statali che si sviluppa nell'arco di due anni e che prevede, anche, un costante monitoraggio della velocità del processo di cambiamento.

In considerazione dei vantaggi che possono derivare a tutta la Pubblica Amministrazione dall'applicazione della presente direttiva si raccomanda di curarne, con tutti i mezzi possibili, la più ampia ed immediata attuazione e di garantirne la massima diffusione a tutti i dipendenti.

Ogni Amministrazione, pertanto, è tenuta a porre in essere le attività necessarie al raggiungimento dell'obiettivo di legislatura, in modo da garantire che, entro la data della sua scadenza, tutte le comunicazioni nelle Pubbliche Amministrazioni possano avvenire esclusivamente in via elettronica.

PARAGRAFO II

Com'è noto, l'utilizzo della posta elettronica quale valido mezzo di trasmissione di documenti informatici è già previsto dall'articolo 14 del Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, approvato con D.P.R. 28/12/2000, n. 445, che consente di utilizzare la posta elettronica quale strumento sostitutivo o integrativo di quelli già ordinariamente utilizzati.

Appare, perciò, necessario che le Pubbliche Amministrazioni provvedano a dotare tutti i dipendenti di una casella di posta elettronica (anche quelli per i quali non sia prevista la dotazione di un personal computer) e ad attivare, inoltre, apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza. Queste ultime dovranno procedere alla tempestiva lettura, almeno una volta al giorno, della corrispondenza ivi pervenuta, adottando gli opportuni metodi di conservazione della stessa in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti.

CARATTERISTICHE

La posta elettronica può essere utilizzata per la trasmissione di tutti i tipi di informazioni, documenti e comunicazioni in formato elettronico e, a differenza di altri mezzi tradizionali, offre

notevoli vantaggi in termini di:
· maggiore semplicità ed economicità di trasmissione, inoltro e riproduzione;
· semplicità ed economicità di archiviazione e ricerca;
· facilità di invio multiplo, cioè a più destinatari contemporaneamente, con costi estremamente più bassi di quelli dei mezzi tradizionali;
· velocità ed asincronia della comunicazione, in quanto non richiede la contemporanea presenza degli interlocutori;
· possibilità di consultazione ed uso anche da postazioni diverse da quella del proprio ufficio, anche al di fuori della sede dell'Amministrazione ed in qualunque momento grazie alla persistenza del messaggio nella sua casella di posta elettronica;
· integrabilità con altri strumenti di automazione di ufficio, quali rubrica, agenda, lista di distribuzione ed applicazioni informatiche in genere.
CONTENUTI
Le singole Amministrazioni, nell'ambito delle rispettive competenze, ferma restando l'osservanza delle norme in materia della riservatezza dei dati personali e delle norme tecniche di sicurezza informatica, si adopereranno per estendere l'utilizzo la posta elettronica, tenendo presente quanto segue:
· è sufficiente ricorrere ad un semplice messaggio di posta elettronica, ad esempio, per richiedere o concedere ferie o permessi, richiedere o comunicare designazioni in comitati, commissioni, gruppi di lavoro o altri organismi, convocare riunioni, inviare comunicazioni di servizio ovvero notizie dirette al singolo dipendente (in merito alla distribuzione di buoni pasto, al pagamento delle competenze, a convenzioni stipulate dall'amministrazione ecc….), diffondere circolari o ordini di servizio;
· unitamente al messaggio di posta elettronica, è anche possibile trasmettere, in luogo di documenti cartacei, documenti amministrativi informatici in merito ai quali tale modalità di trasmissione va utilizzata ordinariamente qualora sia sufficiente conoscere il mittente e la data di invio;
· la posta elettronica è, inoltre, efficace strumento per la trasmissione dei documenti informatici sottoscritti ai sensi della disciplina vigente in materia di firme elettroniche;
· la posta elettronica può essere utilizzata anche per la trasmissione della copia di documenti redatti su supporto cartaceo (copia immagine) con il risultato, rispetto al telefax, di ridurre tempi, costi e risorse umane da impiegare, soprattutto quando il medesimo documento debba, contemporaneamente, raggiungere più destinatari;
· quanto alla certezza della ricezione del suddetto documento da parte del destinatario, il mittente, ove ritenuto necessario, può richiedere al destinatario stesso un messaggio di risposta che confermi l'avvenuta ricezione.
Con l'occasione si fa presente che le Amministrazioni, oltre a dotare tutti i loro dipendenti di una casella di posta elettronica sono chiamate ad adottare ogni iniziativa di sostegno e di formazione per promuovere l'uso della stessa da parte di tutto il personale.

PARAGRAFO III

Come già evidenziato, il Comitato dei Ministri per la Società dell'Informazione ha approvato il finanziamento, a favore delle Amministrazioni statali, del progetto, denominato @P@, che prevede interventi per la diffusione e l'utilizzo degli strumenti telematici in sostituzione dei canali tradizionali di comunicazione. Tale progetto, in fase di avanzata attuazione a cura del Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA), prevede la realizzazione:
- dell'Indice della pubblica amministrazione (che individua gli indirizzi istituzionali della P.A.) e l'attribuzione delle corrispondenti caselle di posta elettronica;
- dell'indirizzario elettronico dei singoli dipendenti (ad uso esclusivamente interno alla P.A.);
- di caselle di posta elettronica certificata;
- di specifici progetti delle amministrazioni, ammessi al previsto cofinanziamento, per la trasformazione delle procedure amministrative che attualmente utilizzano il supporto cartaceo in procedure informatizzate.
Il progetto @P@ prevede che resti affidato alle stesse amministrazioni l'inserimento ed il tempestivo aggiornamento dei dati contenuti nell'indice e nell'indirizzario. Ai fini di una efficace attuazione del progetto è, pertanto, necessario che ogni amministrazione provveda:
- ad inserire, sul sito www.indicepa.gov.it, le informazioni di competenza quali: la struttura organizzativa, le aree organizzative omogenee ed i relativi indirizzi di posta elettronica, nonché

le altre informazioni definite nei documenti tecnici presenti sul medesimo sito, entro e non oltre sessanta giorni dalla data di pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana della presente direttiva;
- ad aggiornare, tempestivamente, le medesime informazioni, in modo da garantire l'affidabilità dell'indirizzo di posta elettronica.
E', infine, necessario che, entro il medesimo termine, sia comunicato al Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA), all'indirizzo apa@cnipa.it, il nominativo ed i recapiti del soggetto cui, nell'ambito di ogni Amministrazione, può farsi riferimento in merito alle predette attività.
Al fine di verificare i risultati attesi in termini di efficienza, efficacia ed economicità, il Centro nazionale per l'informatica è incaricato di effettuare, con cadenza semestrale, un monitoraggio sullo stato di attuazione della presente direttiva. Sarà cura del Centro stesso definire, in raccordo con le amministrazioni in indirizzo, le modalità tecnico operative per l'acquisizione dei dati e delle informazioni relativi al suddetto monitoraggio.
Roma, 27 novembre 2003
IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE
Lucio Stanca
IL MINISTRO PER LA FUNZIONE PUBBLICA
Luigi Mazzella

Direttiva del 18 novembre 2005 (Linee guida per la Pubblica amministrazione digitale)

IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE Vista la legge 23 agosto 1988, n. 400, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri; Vista la legge 7 agosto 1990, n. 241, recante «Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi»; Vista la legge 7 giugno 2000, n. 150, recante «Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni»; Visto il decreto del Presidente delle Repubblica 28 dicembre 2000, n. 445, recante «testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa»; Visto il decreto-legge 14 marzo 2005, n. 35, convertito, con modificazioni, in legge 14 maggio 2005, n. 80, recante «Disposizioni urgenti nell'ambito del Piano di azione per lo sviluppo economico, sociale e territoriale»; Visto il decreto legislativo 28 febbraio 2005, n. 42, che prevede l'istituzione del sistema pubblico di connettività e della rete internazionale della pubblica amministrazione; Visto il decreto legislativo 7 marzo 2005, n. 82, recante «Codice dell'amministrazione digitale», che sancisce e disciplina l'uso delle tecnologie dell'informazione e della comunicazione nell'azione amministrativa; Visto il decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, che disciplina la posta elettronica certificata; Visto il decreto del Presidente del Consiglio dei Ministri del 6 maggio 2005, recante «Delega di funzioni in materia di innovazione e tecnologie» al Ministro senza portafoglio dott. Lucio Stanca; Viste le «Linee guida del Governo per lo sviluppo della società dell'informazione nella legislatura», approvate dal Consiglio dei Ministri in data 31 maggio 2002, nelle quali, tra gli obiettivi da raggiungere prioritariamente, è indicata la diffusione dell'impiego della posta elettronica nella pubblica amministrazione; Vista la direttiva del Ministro per l'innovazione e le tecnologie del 27 novembre 2003 per l'impiego della posta elettronica nelle pubbliche amministrazioni, pubblicata nella Gazzetta Ufficiale del 12 gennaio 2004, n. 8; Vista la direttiva del Ministro per l' innovazione e le tecnologie del 18 dicembre 2003, avente ad oggetto le «Linee guida in materia di digitalizzazione dell'Amministrazione per l'anno 2004», pubblicata nella Gazzetta Ufficiale n. 28 del 4 febbraio 2004; Vista la direttiva del Ministro per l'innovazione e le tecnologie del 4 gennaio 2005 avente ad oggetto «Linee guida in materia di digitalizzazione della pubblica amministrazione per l'anno 2005», pubblicata nella Gazzetta Ufficiale n. 35 del 12 febbraio 2005; Considerato che un maggior impiego delle tecnologie informatiche nelle comunicazioni con i cittadini aumenta l'efficienza delle pubbliche amministrazioni e favorisce notevoli risparmi; Ritenuta la necessità di fornire indicazioni operative alle pubbliche amministrazioni in vista dell'entrata in vigore del citato decreto legislativo n. 82 del 2005; Emana la seguente direttiva:

LINEE GUIDA PER LA PUBBLICA AMMINISTRAZIONE DIGITALE

PREMESSA

La presente direttiva è indirizzata a tutte le amministrazioni dello Stato e agli enti pubblici sottoposti alla vigilanza ministeriale; per le Regioni e gli enti locali e territoriali costituisce un contributo alle determinazioni in materia, nel rispetto della loro autonomia amministrativa ed organizzativa. L'emanazione del decreto legislativo 7 marzo 2005 n. 82, recante «Codice dell'amministrazione digitale» (di seguito indicato come «Codice») e del decreto legislativo del 28 febbraio 2005 n. 42, che ha istituito il «sistema pubblico di connettività» e la «rete internazionale della pubblica amministrazione», segna un determinante passo avanti nel processo di modernizzazione della pubblica amministrazione fornendo gli strumenti normativi necessari a dare al processo di digitalizzazione. La puntuale disciplina di fondamentali istituti quali, ad esempio, le firme elettroniche, il documento informatico, la posta elettronica, la carta nazionale dei servizi e la carta di identità elettronica, attribuisce alla pubblica amministrazione gli strumenti tecnico-giuridici attraverso cui ripensare la propria organizzazione in chiave digitale al fine di fornire a cittadini ed imprese i propri servizi «on line» realizzando, nel contempo, una progressiva riduzione dei costi ed un incremento della efficienza e della trasparenza.

Il «Codice dell'amministrazione digitale» che entrerà in vigore il 1° gennaio 2006 sancisce obblighi e fissa termini in vista dei quali è opportuno che le amministrazioni si preparino adeguatamente. Attraverso un esame generale dei principali istituti trattati dalle richiamate norme, la presente direttiva vuole, pertanto, costituire un momento di riflessione e di stimolo

per questa ulteriore e nuova sfida alla quale tutta la P.A. è chiamata indicando di seguito alcuni punti fondamentali dei quali le amministrazioni dovranno fin d'ora assicurare l'attuazione.

1) COMUNICAZIONE TELEMATICA TRA PUBBLICA AMMINISTRAZIONE E CITTADINI.

L'art. 3 del codice sancisce il principio generale in base al quale i cittadini e le imprese hanno il diritto di «richiedere» e di «ottenere» l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali. Il medesimo principio è ripreso anche dal decreto-legge 14 marzo 2005, n. 35 «Disposizioni urgenti nell'ambito del Piano di azione per lo sviluppo economico, sociale e territoriale», convertito, con modificazioni, nella legge 14 maggio 2005, n. 80 che, al comma 3-quater dell'art. 7, stabilisce l'obbligo per le amministrazioni statali di ricevere nonché inviare, ove richiesto, in via telematica, nel rispetto della normativa vigente, la corrispondenza, i documenti e tutti gli atti relativi ad ogni adempimento amministrativo.

a) Comunicazione esterna e posta elettronica

L'obbligo di comunicare per via telematica con i cittadini e le imprese che lo richiedano presuppone che l'amministrazione si adoperi per rendersi facilmente raggiungibile telematicamente; si rende, pertanto, necessario esporre ed evidenziare adeguatamente, sui siti istituzionali di ogni amministrazione, gli indirizzi di posta elettronica utilizzabili dai cittadini, rendendo facilmente reperibili gli indirizzi di posta elettronica degli uffici competenti per gli atti ed i procedimenti di maggiore interesse, con l'indicazione di quelli abilitati alla posta certificata. Si segnala che le medesime informazioni devono essere inserite anche nel sito www.indicepa.gov.it. Si rammenta inoltre che, ai sensi dell'art. 54 del codice, le amministrazioni sono tenute, fra l'altro, ad evidenziare sul proprio sito i principali procedimenti di competenza indicando gli eventuali termini, il nome del responsabile e l'unità organizzativa responsabile dell'istruttoria, nonché l'elenco dei servizi già disponibili in rete e di quelli di imminente attivazione.

b) Servizi telematici di informazione preventiva

Nell'ottica di una proficua collaborazione tra pubblica amministrazione e cittadino, è utile che le amministrazioni provvedano ad organizzarsi per realizzare servizi di informazione preventiva in modalità telematica, al fine di fornire tempestivamente, per posta elettronica, a coloro che lo abbiano esplicitamente richiesto, informazioni, documenti e notizie in merito a scadenze (amministrative, tributarie, ecc...) o a pagamenti da effettuare, moduli o formulari per richieste o eventuali rinnovi, ecc. L'amministrazione dovrà adeguatamente pubblicizzare tale servizio, non appena attivato. Un ruolo di rilievo potrebbe essere svolto, in tal senso, dagli uffici relazioni con il pubblico, conformemente ai rilevanti compiti affidatigli dalla legge n. 150 del 2000. I cittadini che avranno cura di comunicare il proprio indirizzo di posta elettronica potranno anche ricevere, con congruo anticipo, informazioni relative ai documenti personali e alle licenze che hanno durata predeterminata di cui sono titolari, allorché la relativa validità sia prossima alla scadenza. Riceveranno, altresì, telematicamente i moduli necessari per l'eventuale rinnovo. Sarà opportuno che ogni amministrazione provveda, preliminarmente, ad un'accurata selezione delle informazioni che possono essere fornite a richiesta, in via telematica, organizzandole e classificandole per categorie, quali per esempio: a) informazioni specifiche e documenti d'interesse individuale del cittadino o dell'impresa; b) informazioni relative a comunicazioni istituzionali (es. avviso circa la realizzazione da parte della singola amministrazione di un nuovo servizio); c) informazioni collegate a scadenze o adempimenti da assolvere nei confronti della pubblica amministrazione.

Le amministrazioni dovranno evidenziare, comunque, che il cittadino è tenuto ad assolvere i propri obblighi legati agli adempimenti scadenzati, a prescindere dall'effettiva ricezione della comunicazione da parte dell'amministrazione.

2) COMUNICAZIONE INTERNA ALLE PUBBLICHE AMMINISTRAZIONI.

È stata più volte ribadita, in particolare nella direttiva per l'impiego della posta elettronica nelle pubbliche amministrazioni, datata 27 novembre 2003, pubblicata nella Gazzetta Ufficiale 12 gennaio 2004, n. 8, l'importanza strategica che l'utilizzo intensivo ed esteso della posta elettronica riveste nell'ottica di un cambiamento radicale della pubblica amministrazione. Lo strumento della posta elettronica, inteso come mezzo di comunicazione e trasmissione di documenti, informazioni, dati (sia all'interno della P.A. che nei confronti dei terzi) presenta caratteristiche di economicità, semplicità e velocità di trasmissione, facilità di archiviazione,

possibilità di invio multiplo, integrabilità con altri strumenti ed applicazioni telematiche e infine, di affidabilità. Per tali motivi l'art. 47 del codice sancisce che «Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica», precisando che esse sono valide ai fini del procedimento amministrativo se ne sia verificata la provenienza specificando le modalità che consentono la verifica della «provenienza» delle comunicazioni allo scopo di conferire ad esse efficacia legale certa. Si rammenta inoltre che, dal primo gennaio del 2006, tutte le pubbliche amministrazioni dovranno privilegiare l'uso della posta elettronica come canale di comunicazione anche con i propri dipendenti. Alla luce delle considerazioni svolte, la prosecuzione delle tradizionali forme di comunicazione, nonostante sussista la possibilità di ricorrere alla posta elettronica, configura l'inosservanza di una disposizione di legge e una fattispecie di improprio uso di denaro pubblico.

3) CARTA NAZIONALE DEI SERVIZI

La Carta Nazionale dei Servizi (CNS) è lo strumento informatico che le pubbliche amministrazioni rilasciano ai cittadini per consentire loro di accedere, attraverso la rete, a quei servizi per i quali sia necessaria l'identificazione in rete del soggetto. La CNS è regolamentata ai sensi del decreto del Presidente della Repubblica 2 marzo 2004, n. 117 che ne stabilisce le modalità d'uso e di diffusione. La possibilità di supportare molteplici contenuti la rende strumento di grande utilità. Alcune amministrazioni regionali hanno già utilizzato la CNS, in alcuni casi cumulandone le funzionalità con quelle della Tessera Sanitaria (TS), con notevole vantaggio anche ai fini dell'accesso alle prestazioni mediche ed ospedaliere. Al fine di accelerarne ed armonizzarne la diffusione, si rende opportuno che le pubbliche amministrazioni locali che intendano avviare progetti di emissione della CNS in regioni che abbiano già avviato la diffusione della CNS, in linea con quanto disposto dall'art. 50 del decreto-legge 30 settembre 2003, n. 269, promuovano specifici accordi con la Regione stessa. Tenuto conto che il numero di CNS in circolazione è di oltre dieci milioni e che molte sono in procinto di essere emesse, tutte le pubbliche amministrazioni che erogano servizi in rete devono provvedere - in coerenza con quanto previsto nell'art. 5, comma 2 del decreto del Presidente della Repubblica 2 marzo 2004, n. 117 - a consentire l'accesso ai servizi ai titolari di tutte le CNS, indipendentemente dall'ente di emissione delle stesse. Contestualmente, le amministrazioni sono tenute a dare esplicita pubblicità nei propri siti istituzionali della possibilità di usufruire dei servizi offerti ai cittadini utilizzando la CNS come strumento di accesso. Si segnala che, in attuazione dell'art. 1 commi 192 e seguenti, della legge 30 dicembre 2004, n. 311, (legge finanziaria 2005), e del decreto del Presidente del Consiglio dei Ministri 31 maggio 2005, pubblicato nella Gazzetta Ufficiale 18 giugno 2005, n. 140, il Centro nazionale per l'informatica nella pubblica amministrazione (di seguito Cnipa) è in procinto di stipulare con il vincitore della apposita procedura di gara, un contratto quadro per la fornitura di un quantitativo massimo di 3 milioni di CNS, che consentirà alle amministrazioni l'acquisizione di carte di riconoscimento in rete e dei relativi servizi di gestione con procedure semplificate, con costi ridotti e con la garanzia di controllo della qualità e della rispondenza agli standard di interoperabilità. Si raccomanda alle amministrazioni il ricorso al predetto contratto quadro che la richiamata legge finanziaria prescrive «ai fini del miglioramento della efficienza operativa della pubblica amministrazione e per il contenimento della spesa pubblica».

4) TRANSAZIONI ECONOMICHE ON LINE

Nel corso di questi ultimi anni, in conformità alle direttive del Ministro per l' innovazione e le tecnologie ed in attuazione della prima fase del «Piano nazionale di e-Government», le pubbliche amministrazioni hanno reso disponibili molti servizi on line per cittadini ed imprese, taluni dei quali prevedono anche il versamento di una somma di denaro (a titolo di pagamento di tasse, imposte, contributi, diritti di segreteria ecc. ...). Tuttavia, soltanto alcune amministrazioni hanno reso possibile l'effettuazione di tali pagamenti in modalità telematica. È, quindi, necessario che le pubbliche amministrazioni consentano all'utente, nell'ambito della medesima procedura telematica, l'effettuazione del pagamento, a qualunque titolo ad esse dovuto. È, peraltro, auspicabile che sia prevista l'utilizzazione di una pluralità di canali di pagamento elettronico per fornire agli utenti la libera scelta tra diverse opzioni (internet, sportelli bancomat ecc. ...). Al fine di semplificare le operazioni di contabilizzazione e controllo dei pagamenti effettuati è opportuno che essi siano univocamente identificabili attraverso un codice, generato automaticamente, che individui l'ente cui il pagamento è diretto, la tipologia di pagamento (tributi, contributi, diritti, ecc. ...) e la data del pagamento. Ai fini della corretta

autenticazione dell'utente potranno essere utilizzate la Carta nazionale dei servizi o la Carta di identità elettronica, strumenti che garantiscono anche il necessario livello di sicurezza. Al fine di incentivare i pagamenti in modalità telematica ed in considerazione dei risparmi gestionali che ne possono derivare, le amministrazioni dovranno ricercare soluzioni che consentano di contenerne il costo a carico dell'utente entro limiti massimi non superiori a quelli di altri mezzi di pagamento.

5) Conferenza di servizi on line

La conferenza di servizi, disciplinata dalla legge 7 agosto 1990, n. 241, costituisce un nodo centrale della semplificazione del procedimento amministrativo essendo il luogo ideale in cui competenze ed interessi diversi vengono ad essere rappresentati trovando il necessario raccordo e coordinamento. Si tratta di un modulo organizzativo volto a consentire la partecipazione al medesimo procedimento di diverse amministrazioni ed enti che, in un'unica sede ed in tempi rapidi, giungono all'adozione di un unico provvedimento amministrativo condiviso. La recente modifica della legge n. 241/1990, operata dalla legge 11 febbraio 2005, n. 15, ha significativamente inciso sulla sua disciplina, semplificandone ulteriormente le modalità di svolgimento ed introducendo, tra le novità più rilevanti, la possibilità di effettuare la conferenza di servizi attraverso l'uso dell'informatica. Il comma 5-bis dell'art. 14 della legge n. 241/1990, peraltro, richiamato dall'art. 41, comma 3, del codice afferma, infatti, che «previo accordo tra le amministrazioni coinvolte, la conferenza dei servizi è convocata e svolta avvalendosi degli strumenti informatici disponibili, secondo i tempi e le modalità stabiliti dalle amministrazioni medesime». Il quadro normativo attuale e la varietà di strumenti tecnologici disponibili consentono già alla P.A. di svolgere la propria attività in modo più efficiente ed efficace; l'uso dell'informatica per la conferenza di servizi consente anche il superamento dei vincoli spaziali e temporali, facilitando ulteriormente il raccordo tra le amministrazioni con conseguente riduzione dei tempi e dei costi. Infatti, attraverso l'uso degli strumenti informatici, le pubbliche amministrazioni coinvolte in un unico procedimento amministrativo potranno essere convocate e partecipare ad una conferenza di servizi assicurando la contemporanea partecipazione alle riunioni dei loro rappresentanti, anche da un luogo diverso dalla sede dell'amministrazione procedente, virtualmente unite dal contemporaneo utilizzo di collegamenti telematici (conferenza svolta in modalità sincrona) ovvero, collegandosi al tavolo virtuale della conferenza in tempi diversi (conferenza svolta in modalità asincrona). La scelta riguardo alla modalità ritenuta più adeguata alla singola fase ed alla tipologia di conferenza e di interessi coinvolti è demandata all'accordo preventivamente raggiunto dalle medesime amministrazioni. Si precisa che, nell'ambito delle proprie competenze, il Cnipa è stato incaricato di predisporre un'apposita procedura informatica utilizzabile da tutte le amministrazioni pubbliche ed in grado di consentire la convocazione e l'effettuazione delle conferenze di servizi in modo semplice ed univoco, nel pieno rispetto della normativa vigente. Detta procedura, basata sull'uso di strumenti informatici di larga diffusione (posta elettronica, sistemi di chatting, forum, video o teleconferenza, ecc. ...), consentirà l'adeguamento alle specifiche fasi ed esigenze di ogni conferenza. Attraverso una specifica sperimentazione saranno verificate sul campo tutte le funzionalità della piattaforma in modo da renderne omogenea ed uniforme l'applicazione. Le economie scaturenti dall'uso della suddetta piattaforma realizzeranno l'ulteriore obiettivo di rendere la conferenza di servizi uno dei più efficaci strumenti di semplificazione e razionalizzazione dell'azione amministrativa.

6) SICUREZZA DEI SISTEMI INFORMATIVI

Lo sviluppo della comunicazione telematica con cittadini e imprese e la conseguente necessità di operare sulla rete rendono essenziale l'adozione di adeguate misure di sicurezza informatica per rispondere all'esigenza di garantire riservatezza e integrità dei contenuti, continuità e disponibilità dei servizi. Si richiamano le seguenti disposizioni del codice la cui attuazione richiede particolari cautele dal punto di vista della sicurezza informatica: l'art. 5 (Effettuazione dei pagamenti con modalità informatiche), l'art. 51 (Sicurezza dei dati), l'art. 57 (Moduli e formulari); non vanno sottovalutati, inoltre, gli aspetti relativi alla sicurezza in relazione agli articoli 31 (Obblighi di sicurezza) e 34 (Trattamento con strumenti elettronici) del decreto legislativo «Codice in materia di protezione dei dati personali». È, pertanto, necessario che le pubbliche amministrazioni statali che non vi abbiano già provveduto, attuino quanto già previsto nella direttiva sulla sicurezza informatica e delle telecomunicazioni del 16 gennaio 2002 che, all'allegato 2, prevede che esse definiscano, progettino e realizzino, misure relative:
– all'organizzazione della sicurezza (al riguardo vedasi anche l'art. 17 del codice, «Strutture

per l'organizzazione, l' innovazione e le tecnologie»); – alla gestione della sicurezza; – all'analisi e gestione del rischio; – al controllo fisico/logico degli accessi; – alla protezione antivirus; – alla gestione dei supporti; tenendo conto, altresì, delle indicazioni del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni raccolte nell'apposito documento «Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la pubblica amministrazione» consultabile sui siti www.innovazione.gov.it e www.cnipa.gov.it

7) STRUTTURE PER L'ORGANIZZAZIONE, L' INNOVAZIONE E LE TECNOLOGIE

Infine, si rammenta che le amministrazioni statali, ai sensi dell'art. 17 del codice, per garantire l'attuazione delle disposizioni normative e delle direttive volte alla riorganizzazione e alla digitalizzazione della P.A., devono individuare un «centro di competenza» interno cui afferiscano, tra l'altro, i compiti di coordinamento strategico dello sviluppo dei sistemi informativi, di indirizzo, coordinamento e monitoraggio dello sviluppo dei servizi sia interni che esterni, di analisi e cooperazione alla revisione della organizzazione dell'amministrazione, di garanzia della coerenza tra l'organizzazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, nonché di promozione delle iniziative necessarie ad assicurare la più rapida attuazione della presente direttiva. Si sottolinea che la norma usa la generica espressione «centro di competenza» affinché ciascuna amministrazione possa identificarlo nella struttura organizzativa (Direzione, Dipartimento, Ufficio, ecc..) ritenuta più idonea nell'ambito della propria organizzazione, anche in considerazione del fatto che presso varie pubbliche amministrazioni esistono già strutture cui sono demandate tali funzioni. La presente direttiva sarà inviata ai competenti organi di controllo e sarà pubblicata nella Gazzetta Ufficiale della Repubblica italiana. Roma, 18 novembre 2005 Il Ministro: Stanca Registrata alla Corte dei conti il 29 dicembre 2005 Ministeri istituzionali - Presidenza del Consiglio dei Ministri, registro n. 14, foglio n. 32

Codice dell'amministrazione digitale: art. 6 (Capo I), artt. 45 e seguenti (Capo IV)

ART. 6 (Utilizzo della posta elettronica certificata)

1. Per le comunicazioni di cui all' articolo 48, comma 1 , con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano la posta elettronica certificata. La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano .

1-bis. La consultazione degli indirizzi di posta elettronica certificata, di cui agli articoli 16, comma 10, e 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185 , convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2 , e l'estrazione di elenchi dei suddetti indirizzi, da parte delle pubbliche amministrazioni è effettuata sulla base delle regole tecniche emanate da DigitPA, sentito il Garante per la protezione dei dati personali .

ART. 45 (Valore giuridico della trasmissione)

1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale .

2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore

ART. 46 (Dati particolari contenuti nei documenti trasmessi)

1. Al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196 , i documenti informatici trasmessi ad altre pubbliche amministrazioni per via telematica possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite.

ART. 47 (Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni)

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

1-bis. L'inosservanza della disposizione di cui al comma 1, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare.

2. Ai fini della verifica della provenienza le comunicazioni sono valide se:

a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;

b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71. E' in ogni caso esclusa la trasmissione di documenti a mezzo fax;

d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

3. Le pubbliche amministrazioni e gli altri soggetti di cui all'articolo 2, comma 2, provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo. La pubbliche amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

ART. 48 (Posta elettronica certificata)

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA.
2. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi al decreto del Presidente del Consiglio dei Ministri di cui al comma 1.

ART. 49 (Segretezza della corrispondenza trasmessa per via telematica)

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.
2. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Linee guida per posta elettronica e internet (Linee guida del Garante della privacy, pubblicate sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007)

Registro delle deliberazioni
Del. n. 13 del 1° marzo 2007

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 dott. 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 artt. 24 e 154, comma 1, lett. b) e c) del Codice in materia di protezione dei dati personali (d.lg. 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 (*artt. 15, 31 ss., 167 e 169 del Codice*);
c) emerge l'esigenza di tutelare i lavoratori interessati anche perché 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)]

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. [(2)]

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 (*artt. 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*). [(3)]

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 (*artt. 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 (*artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 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, lett. b) Codice dell'amministrazione digitale*). [(4)]

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; par. 5.2*);
b) il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (*art. 11, comma 1, lett. 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. par. 3*);
c) i trattamenti devono essere effettuati per finalità *determinate*, *esplicite* e *legittime* (*art. 11, comma 1, lett. b), del Codice: par. 4 e 5*), osservando il principio di *pertinenza* e *non eccedenza* (*par. 6*). Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti (*par. 8*) ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"* (***Parere n. 8/2001***, *cit., punti 5 e 12*).

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, par. 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"*). [(5)]

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, l. 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, lett. 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. artt. 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, l. 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. [(6)]

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. É 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. [(7)] A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (*art. 11, comma 2, del Codice*). [(8)]

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. [(9)] Ciò, anche in presenza di attività di controllo discontinue. [(10)]

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 [(11)], nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. [(12)]

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 *(artt. 3, 11, comma 1, lett. 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; (13)
- 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 technologies–PETs*). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., 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'attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (*art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Provv.* ***2 febbraio 2006****, cit.*).

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

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi 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 es., 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 (*artt. 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*). (14)

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").

É 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, etc.), 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; (15)
- 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 es., 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. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica. (16) In caso di eventuali assenze non programmate (ad es., 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 es., 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, lett. 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 nn. **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:

a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (*art. 24, comma 1, lett. f) del Codice*);
b) in caso di valida manifestazione di un libero consenso;
c) 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, lett. 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 (*artt. 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, lett. 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, lett. 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.) affinché, 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, lett. 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, lett. 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 sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell'art. 143, comma 2, del Codice.

Roma, 1° marzo 2007

IL PRESIDENTE
Pizzetti

IL RELATORE
Paissan

IL SEGRETARIO GENERALE
Buttarelli

---

(1) Cfr. Gruppo Art. 29 sulla protezione dei dati, **Parere n. 8/2001** sul trattamento dei dati personali nel contesto dell'occupazione, 13 settembre 2001, punti 5 e 12, in **http://ec.europa.eu/...pdf**.

(2) Cfr. Niemitz v. Germany, 23 novembre 1992, par. 29; v. pure Halford v. United Kingdom, 25 giugno 1997, parr. 44-46.

(3) V. pure Gruppo Art. 29 cit., Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, Wp 55, 29 maggio 2002, p. 4, in **http://ec.europa.eu/...pdf** .

(4) V. pure la Direttiva per l'impiego della posta elettronica nelle pubbliche amministrazioni del 27 novembre 2003; Raccomandazione n. R (89)2 del Consiglio d'Europa in materia di protezione dei dati personali nel contesto del rapporto di lavoro, in **http://cm.coe.int/...doc**); **Parere n. 8/2001** , cit., punto 5.

(5) V. altresì la Raccomandazione n. R (89) 2, cit., punto 3; **Parere n. 8/2001** , cit., punto 9.1 e Wp 55, cit., punto 3.1.3.

(6) Cass. 18 febbraio 1983, n. 1236 e 16 settembre 1997, n. 9211.

(7) Cfr. Cass. 11 marzo 1986, n. 1490.

(8) Cfr. anche Cass., 17 giugno 2000, n. 8250 rispetto all'uso probatorio.

(9) Cass. 18 febbraio 1983, n. 1236 e 16 settembre 1997, n. 9211.

(10) Cass. 11 marzo 1986, n. 1490 cit.

(11) Raccomandazione n. R (89)2, cit., art. 3, comma 1.

(12) Raccomandazione n. R (89)2, art. 3, comma 2; disposizione in base alla quale, in presenza di rischi "per il diritto al rispetto della vita privata e della dignità umana dei lavoratori, dovrà essere ricercato l'accordo dei lavoratori o dei loro rappresentanti prima dell'introduzione o della modifica di tali sistemi o procedimenti, a meno che altre garanzie specifiche non siano previste dalla legislazione nazionale": art. 3, comma 3.

(13) Cfr. **Provv. 2 febbraio 2006** , in , doc. web n. **1229854**.

(14) Cfr. nota del **Garante 16 giugno 1999** , **Boll. n. 9, giugno 1999** , p. 96; Tar Lazio, Sez. I ter, 15 novembre 2001, n. 9425.

(15) Cfr. il documento Wp 55, cit., p. 23.

(16) Cfr. il documento Wp 55, cit., p. 5.

Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro (Direttiva della Presidenza del Consiglio dei ministri - Dipartimento della Funzione pubblica N. 02/09 del 26 maggio 2009)

Alle Amministrazioni pubbliche di cui all'art. 1, comma 2, del d.lgs. n. 165 del 2001

Oggetto: Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro.

PREMESSA
Le risorse ICT costituiscono, ormai da tempo, il principale strumento di lavoro posto a disposizione dei dipendenti delle pubbliche amministrazioni. L'ampia distribuzione di tali risorse tra i dipendenti ne favorisce il diffuso utilizzo anche per finalità diverse da quelle lavorative. La prassi, ancorché ben conosciuta dalle Amministrazioni, è difficile da monitorare, sia per il costo dell'eventuale attività di monitoraggio, sia per le implicazioni relative alla tutela della riservatezza e dei dati personali. D'altronde, tale utilizzo non istituzionale non provoca, di norma, costi aggiuntivi, tenuto conto della modalità di pagamento "flat" (non riferita, pertanto, al consumo) utilizzata nella generalità dei casi dalle Amministrazioni per l'utilizzo di quasi tutte le risorse ICT (postazioni di lavoro, connessioni di rete e posta elettronica). In considerazione della delicatezza della materia, che tocca i diritti individuali (quale il diritto alla segretezza della corrispondenza) e richiede, pertanto, un giusto bilanciamento con il potere di controllo dell'Amministrazione, si ritiene opportuno fornire indicazioni utili a facilitare, da un lato, il corretto utilizzo degli strumenti ICT da parte dei dipendenti e, dall'altro, il proporzionato esercizio del potere datoriale di controllo da parte delle Amministrazioni in indirizzo.

1. Esercizio del potere di controllo e doveri di comportamento dei dipendenti delle pubbliche amministrazioni
Le Pubbliche Amministrazioni, in quanto datori di lavoro, sono tenute ad assicurare la funzionalità ed il corretto impiego degli strumenti ICT da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi. Nell'esercizio del potere di controllo, le Amministrazioni devono attenersi ad alcune regole e principi generali: - innanzitutto deve essere rispettato il principio di proporzionalità, che si concreta nella pertinenza e non eccedenza delle attività di controllo. Le limitazioni della libertà e dei diritti individuali devono, infatti, essere proporzionate allo scopo perseguito; è in ogni caso esclusa l'ammissibilità di controlli prolungati, costanti e indiscriminati; - inoltre, l'introduzione di tecnologie e di strumenti per il controllo sull'uso della rete e della posta elettronica deve essere fatto rispettando le procedure di informazione/consultazione delle rappresentanze dei lavoratori previste dai contratti collettivi; - infine, i lavoratori devono essere preventivamente informati dell'esistenza di dispositivi di controllo atti a raccogliere i dati personali. A fronte del potere di controllo dell'Amministrazione datore di lavoro, esiste in capo ai dipendenti l'obbligo, sancito da norme di legge (anche di rilevanza penale) e di contratto, di adottare comportamenti conformi al corretto espletamento della prestazione lavorativa ed idonei a non causare danni o pericoli ai beni mobili ed agli strumenti ad essi affidati, tra i quali vi sono le attrezzature ICT ed i sistemi informativi messi a disposizione dall'Amministrazione. Al riguardo, si ritiene opportuno ricordare, oltre alle disposizioni del Codice disciplinare contenuto nei contratti collettivi di comparto (che dispongono sanzioni in caso di *"negligenza nella cura dei locali e dei beni mobili o strumenti a lui affidati o sui quali, in relazione alle sue responsabilità, debba espletare azione di vigilanza"*), anche il dettato del Codice di comportamento dei dipendenti delle pubbliche amministrazioni di cui al Decreto del Ministro per la funzione pubblica del 28 novembre 2000 che, ove richiamato dal Codice disciplinare dei CCNL dei

diversi comparti, costituisce, oltre che norma di valenza etico-comporamentale, anche vero e proprio obbligo la cui inosservanza da parte dei dipendenti è passibile di sanzione. In particolare, l'art. 10, comma 3, del Codice di comportamento dispone che *"Il dipendente non utilizza a fini privati materiale o attrezzature di cui dispone per ragioni di ufficio."* Pertanto, l'utilizzo delle risorse ICT da parte dei dipendenti, oltre a non dover compromettere la sicurezza e la riservatezza del Sistema informativo, non deve pregiudicare ed ostacolare le attività dell'Amministrazione od essere destinato al perseguimento di interessi privati in contrasto con quelli pubblici. Anche la giurisprudenza, in particolare quella della Corte dei conti (tra le altre, Sez. giurisd. Piemonte, sent. 1856/2003, e Sez. giurisd. Basilicata, sent. n. 83/2006), ha sanzionato l'indebito utilizzo della connessione ad internet da parte di un dipendente, statuendo che essa configura profili di responsabilità a carico del medesimo per il danno patrimoniale cagionato all'Amministrazione, consistente nel mancato svolgimento della prestazione lavorativa durante le ore di connessione. Con riferimento al potere di controllo, la Corte ha, inoltre, osservato come, a seguito di ripetute e significative anomalie (rilevate, ad esempio, per la presenza di virus provenienti da siti non istituzionali), l'Amministrazione possa svolgere verifiche ex post sui dati inerenti l'accesso alla rete dei propri dipendenti. Per adempiere il proprio dovere di diligenza e vigilanza nell'utilizzo dei beni e strumenti ad esso affidati, il dipendente ha, pertanto, anche l'obbligo di impedire ad altri indebiti utilizzi della propria apparecchiatura informatica, non rilevando, al fine del difetto di responsabilità, il fatto che altri, in sua assenza, abbia potuto usare la postazione lavorativa. In difetto, il comportamento del dipendente si configura come negligente, inescusabile e gravemente colposo.

2. I principi contenuti nelle linee guida del Garante della protezione dei dati personali

Con deliberazione del 1° marzo 2007, n. 13 (pubblicato in G.U. n. 58 del 10 marzo 2007), il Garante della protezione dei dati personali ha fornito le linee guida per l'utilizzo nei luoghi di lavoro della posta elettronica e di internet. Allo stato, lasciando da parte i profili di illecito penale e/o disciplinare sopra richiamati, tale deliberazione costituisce, in particolare per quanto attiene alla disciplina del trattamento dei dati, sicuro punto di riferimento e regolamentazione delle modalità di utilizzo del Sistema informativo delle pubbliche amministrazioni da parte dei dipendenti nell'ambito del rapporto di lavoro. La deliberazione, nel definire, per i datori di lavoro, le regole in materia di trattamento dei dati personali raccolti in occasione delle attività di verifica del corretto utilizzo della rete Internet e del sistema di posta elettronica da parte dei lavoratori, fissa dei principi che non riguardano esclusivamente la tutela della privacy ma riprendono anche le disposizioni contenute nel "Codice dell'amministrazione digitale" (decreto legislativo 7 marzo 2005, n. 82 pubblicato in G.U. del 16 maggio 2005, n. 112 - S.O. n. 93, aggiornato dal d.lgs. n. 159 del 4 aprile 2006, pubblicato in G.U. del 29 aprile 2006, n. 99 - S.O. n. 105 recante "Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82 recante codice dell'amministrazione digitale"). In particolare, come definito anche dalle linee guida del Garante, il datore di lavoro (secondo i poteri a lui affidati dalle norme del codice civile, articoli 2086, 2087 e 2104), può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro. Nell'esercizio di tali prerogative, tuttavia, deve rispettare la libertà e la dignità dei lavoratori, tenendo presente, al riguardo, quanto disposto dalle norme poste a tutela del lavoratore (ci si riferisce, in particolare, al divieto di installare *"apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"* di cui all'art. 4 della legge n. 300 del 1970). Inoltre, secondo i richiamati principi di pertinenza e non eccedenza, i mezzi e l'ampiezza del controllo devono essere proporzionati allo scopo: in base a tale considerazione il datore di lavoro potrebbe, ad esempio, verificare se vi è stato indebito utilizzo della connessione ad internet da parte del dipendente attraverso il controllo degli accessi e dei tempi di connessione, senza però indagare sul contenuto dei siti visitati. I lavoratori devono essere posti in grado di conoscere quali sono le attività consentite, a quali controlli sono sottoposti, le modalità del trattamento dei dati e in quali sanzioni

possono incorrere nel caso di abusi. Al riguardo, viene raccomandata l'adozione di un disciplinare interno adeguatamente pubblicizzato e di idonee misure di tipo organizzativo.

3. Utilizzo della rete internet
In capo all'Amministrazione datore di lavoro, alla cui proprietà è riconducibile il Sistema informativo (ivi inclusi le apparecchiature, i programmi ed i dati inviati, ricevuti e salvati), è posto l'onere di predisporre misure per ridurre il rischio di usi impropri di internet, consistenti in attività non correlate alla prestazione lavorativa, quali la visione di siti non pertinenti, l'upload e il download di files, l'uso di servizi di rete con finalità ludiche o comunque estranee all'attività lavorativa. A tale proposito, si raccomanda alle Amministrazioni di dotarsi di software idonei ad impedire l'accesso a siti internet aventi contenuti e/o finalità vietati dalla legge. Inoltre, l'Amministrazione, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva ed, eventualmente, anche dei diversi profili professionali autorizzati all'uso della rete, potrà adottare una o più delle misure indicate dalla citata deliberazione del Garante della privacy che, a mero titolo riepilogativo, si riportano di seguito: - 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 es., 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. Tuttavia, l'utilizzo di internet per svolgere attività che non rientrano tra i compiti istituzionali potrebbe essere regolamentato e, quindi, consentito ai dipendenti per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad esempio, per effettuare adempimenti *on line* nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi). Tale modalità, purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni, avrebbe, inoltre, il vantaggio di contribuire a ridurre gli spostamenti delle persone e gli oneri logistici e di personale per l'amministrazione che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi.

4. Utilizzo della posta elettronica istituzionale Con riferimento all'utilizzo della casella di posta elettronica istituzionale deve osservarsi che il contenuto dei messaggi, come pure i file allegati e i dati esteriori delle comunicazioni, 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 (qual è anche il luogo di lavoro); un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, comma 4, c.p.[*] ; art. 49 Codice dell'amministrazione digitale). Al fine di contemperare le esigenze di corretto ed ordinato svolgimento della vita lavorativa e di prevenzione di inutili intrusioni nella sfera personale dei lavoratori e di violazioni della segretezza della corrispondenza, sarebbe, pertanto, opportuno che le Amministrazioni esplicitassero regole e strumenti per l'utilizzo della posta elettronica. Ciò consentirebbe, infatti, di evitare, ovvero almeno limitare, l'insorgere di difficoltà in ordine all'utilizzo della posta elettronica poiché, per la configurazione stessa dell'indirizzo *e-mail*, nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta operando quale espressione dell'Amministrazione o ne faccia, invece, un uso personale pur restando nell'ambito lavorativo istituzionale.
Si invitano, pertanto, le Amministrazioni in indirizzo, attraverso i dirigenti responsabili, ad attuare tutte le misure di informazione, controllo e verifica consentite al fine regolamentare la fruizione delle risorse ICT e responsabilizzare i dipendenti nei confronti di eventuali utilizzi non coerenti con

la prestazione lavorativa e non conformi alle norme che disciplinano il lavoro alle dipendenze delle pubbliche amministrazioni.

IL MINISTRO PER LA PUBBLICA AMMINISTRAZIONE E L'INNOVAZIONE
Renato Brunetta

[*] Reato di violazione, sottrazione e soppressione di corrispondenza: *"Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza"*.

Posta elettronica certificata

Decreto del Presidente della Repubblica 11 febbraio 2005, n.68 (Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3.)

IL PRESIDENTE DELLA REPUBBLICA
- Visto l'articolo 87 della Costituzione;
- Visto l'articolo 15, comma 2, della legge 15 marzo 1997, n. 59;
- Visto l'articolo 27, commi 8, lettera e), e 9, della legge 16 gennaio 2003, n. 3;
- Visto l'articolo 17, comma 2, della legge 23 agosto 1988, n. 400;
- Visto l'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione del 25 marzo 2004;
- Espletata la procedura di informazione di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, attuata con legge 21 giugno 1986, n. 317, cosi' come modificata dal decreto legislativo 23 novembre 2000, n. 427;
- Acquisito il parere della Conferenza unificata, ai sensi dell'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, espresso nella riunione del 20 maggio 2004;
- Vista la nota del 29 marzo 2004, con la quale e' stato richiesto il parere del Garante per la protezione dei dati personali;
- Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 14 giugno 2004;
- Acquisito il parere delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;
- Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 28 gennaio 2005;
- Sulla proposta del Ministro per la funzione pubblica e del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze;

EMANA

il seguente regolamento:

Articolo 1 - Oggetto e definizioni

1. Il presente regolamento stabilisce le caratteristiche e le modalità per l'erogazione e la fruizione di servizi di trasmissione di documenti informatici mediante posta elettronica certificata.
2. Ai fini del presente regolamento si intende per:
a. busta di trasporto, il documento informatico che contiene il messaggio di posta elettronica certificata;
b. Centro nazionale per l'informatica nella pubblica amministrazione, di seguito denominato: «CNIPA», l'organismo di cui all'articolo 4, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, come modificato dall'articolo 176, comma 3, del decreto legislativo 30 giugno 2003, n. 196;
c. dati di certificazione, i dati inseriti nelle ricevute indicate dal presente regolamento, relativi alla trasmissione del messaggio di posta elettronica certificata;
d. dominio di posta elettronica certificata, l'insieme di tutte e sole le caselle di posta elettronica certificata il cui indirizzo fa riferimento, nell'estensione, ad uno stesso dominio della rete Internet, definito secondo gli standard propri di tale rete;
e. log dei messaggi, il registro informatico delle operazioni relative alle trasmissioni effettuate mediante posta elettronica certificata tenuto dal gestore;
f. messaggio di posta elettronica certificata, un documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati;
g. posta elettronica certificata, ogni sistema di posta elettronica nel quale e' fornita

al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici;
h. posta elettronica, un sistema elettronico di trasmissione di documenti informatici;
i. riferimento temporale, l'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata;
l. utente di posta elettronica certificata, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi ente, associazione o organismo, nonche' eventuali unità organizzative interne ove presenti, che sia mittente o destinatario di posta elettronica certificata;
m. virus informatico, un programma informatico avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.

Articolo 2 - Soggetti del servizio di posta elettronica certificata

1. Sono soggetti del servizio di posta elettronica certificata:
a. il mittente, cioè l'utente che si avvale del servizio di posta elettronica certificata per la trasmissione di documenti prodotti mediante strumenti informatici;
b. il destinatario, cioè l'utente che si avvale del servizio di posta elettronica certificata per la ricezione di documenti prodotti mediante strumenti informatici;
c. il gestore del servizio, cioè il soggetto, pubblico o privato, che eroga il servizio di posta elettronica certificata e che gestisce domini di posta elettronica certificata.

Articolo 3 - Trasmissione del documento informatico

1. Il comma 1 dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e' sostituito dal seguente: «1. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.».

Articolo 4 - Utilizzo della posta elettronica certificata

1. La posta elettronica certificata consente l'invio di messaggi la cui trasmissione e' valida agli effetti di legge.
2. Per i privati che intendono utilizzare il servizio di posta elettronica certificata, il solo indirizzo valido, ad ogni effetto giuridico, e' quello espressamente dichiarato ai fini di ciascun procedimento con le pubbliche amministrazioni o di ogni singolo rapporto intrattenuto tra privati o tra questi e le pubbliche amministrazioni. Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma.
3. La volontà espressa ai sensi del comma 2 non può comunque dedursi dalla mera indicazione dell'indirizzo di posta certificata nella corrispondenza o in altre comunicazioni o pubblicazioni del soggetto.
4. Le imprese, nei rapporti tra loro intercorrenti, possono dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese. Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma.
5. Le modalità attraverso le quali il privato comunica la disponibilità all'utilizzo della posta elettronica certificata, il proprio indirizzo di posta elettronica certificata, il mutamento del medesimo o l'eventuale cessazione della disponibilità, nonché le modalità di conservazione, da parte dei gestori del servizio, della documentazione relativa sono definite nelle regole tecniche di cui all'articolo 17.
6. La validità della trasmissione e ricezione del messaggio di posta elettronica certificata e' attestata rispettivamente dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna, di cui all'articolo 6.
7. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono di uno dei gestori di cui agli articoli 14 e 15.

Articolo 5 - Modalità della trasmissione e interoperabilità

1. Il messaggio di posta elettronica certificata inviato dal mittente al proprio gestore di posta elettronica certificata viene da quest'ultimo trasmesso al destinatario direttamente o trasferito al gestore di posta elettronica certificata di cui si avvale il

destinatario stesso; quest'ultimo gestore provvede alla consegna nella casella di posta elettronica certificata del destinatario.
2. Nel caso in cui la trasmissione del messaggio di posta elettronica certificata avviene tra diversi gestori, essi assicurano l'interoperabilità dei servizi offerti, secondo quanto previsto dalle regole tecniche di cui all'articolo 17.

Articolo 6 - Ricevuta di accettazione e di avvenuta consegna

1. Il gestore di posta elettronica certificata utilizzato dal mittente fornisce al mittente stesso la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione di un messaggio di posta elettronica certificata.
2. Il gestore di posta elettronica certificata utilizzato dal destinatario fornisce al mittente, all'indirizzo elettronico del mittente, la ricevuta di avvenuta consegna.
3. La ricevuta di avvenuta consegna fornisce al mittente prova che il suo messaggio di posta elettronica certificata e' effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario e certifica il momento della consegna tramite un testo, leggibile dal mittente, contenente i dati di certificazione.
4. La ricevuta di avvenuta consegna può contenere anche la copia completa del messaggio di posta elettronica certificata consegnato secondo quanto specificato dalle regole tecniche di cui all'articolo 17.
5. La ricevuta di avvenuta consegna e' rilasciata contestualmente alla consegna del messaggio di posta elettronica certificata nella casella di posta elettronica messa a disposizione del destinatario dal gestore, indipendentemente dall'avvenuta lettura da parte del soggetto destinatario.
6. La ricevuta di avvenuta consegna e' emessa esclusivamente a fronte della ricezione di una busta di trasporto valida secondo le modalità previste dalle regole tecniche di cui all'articolo 17.
7. Nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi di posta elettronica certificata inviati, le informazioni di cui all'articolo 11, detenute dai gestori, sono opponibili ai terzi ai sensi dell'artico lo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

Articolo 7 - Ricevuta di presa in carico

1. Quando la trasmissione del messaggio di posta elettronica certificata avviene tramite più gestori il gestore del destinatario rilascia al gestore del mittente la ricevuta che attesta l'avvenuta presa in carico del messaggio.

Articolo 8 - Avviso di mancata consegna

1. Quando il messaggio di posta elettronica certificata non risulta consegnabile il gestore comunica al mittente, entro le ventiquattro ore successive all'invio, la mancata consegna tramite un avviso secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

Articolo 9 - Firma elettronica delle ricevute e della busta di trasporto

1. Le ricevute rilasciate dai gestori di posta elettronica certificata sono sottoscritte dai medesimi mediante una firma elettronica avanzata ai sensi dell'articolo 1, comma 1, lettera dd), del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, generata automaticamente dal sistema di posta elettronica e basata su chiavi asimmetriche a coppia, una pubblica e una privata, che consente di rendere manifesta la provenienza, assicurare l'integrità e l'autenticità delle ricevute stesse secondo le modalità previste dalle regole tecniche di cui all'articolo 17.
2. La busta di trasporto e' sottoscritta con una firma elettronica di cui al comma 1 che garantisce la provenienza, l'integrità e l'autenticità del messaggio di posta elettronica certificata secondo le modalità previste dalle regole tecniche di cui all'articolo 17.

Articolo 10 - Riferimento temporale

1. Il riferimento temporale e la marca temporale sono formati in conformità a quanto previsto dalle regole tecniche di cui all'articolo 17.
2. I gestori di posta elettronica certificata appongono un riferimento temporale su ciascun messaggio e quotidianamente una marca temporale sui log dei messaggi.

Articolo 11 - Sicurezza della trasmissione

1. I gestori di posta elettronica certificata trasmettono il messaggio di posta elettronica certificata dal mittente al destinatario integro in tutte le sue parti, includendolo nella

busta di trasporto.
2. Durante le fasi di trasmissione del messaggio di posta elettronica certificata, i gestori mantengono traccia delle operazioni svolte su un apposito log dei messaggi. I dati contenuti nel suddetto registro sono conservati dal gestore di posta elettronica certificata per trenta mesi.
3. Per la tenuta del registro i gestori adottano le opportune soluzioni tecniche e organizzative che garantiscano la riservatezza, la sicurezza, l'integrità e l'inalterabilità nel tempo delle informazioni in esso contenute.
4. I gestori di posta elettronica certificata prevedono, comunque, l'esistenza di servizi di emergenza che in ogni caso assicurano il completamento della trasmissione ed il rilascio delle ricevute.

Articolo 12 - Virus informatici

1. Qualora il gestore del mittente riceva messaggi con virus informatici e' tenuto a non accettarli, informando tempestivamente il mittente dell'impossibilità di dar corso alla trasmissione; in tale caso il gestore conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'articolo 17.
2. Qualora il gestore del destinatario riceva messaggi con virus informatici e' tenuto a non inoltrarli al destinatario, informando tempestivamente il gestore del mittente, affinche' comunichi al mittente medesimo l'impossibilità di dar corso alla trasmissione; in tale caso il gestore del destinatario conserva i messaggi ricevuti per trenta mesi secondo le modalità definite dalle regole tecniche di cui all'articolo 17.

Articolo 13 - Livelli minimi di servizio

1. I gestori di posta elettronica certificata sono tenuti ad assicurare il livello minimo di servizio previsto dalle regole tecniche di cui all'articolo 17.

Articolo 14 - Elenco dei gestori di posta elettronica certificata

1. Il mittente o il destinatario che intendono fruire del servizio di posta elettronica certificata si avvalgono dei gestori inclusi in un apposito elenco pubblico disciplinato dal presente articolo.
2. Le pubbliche amministrazioni ed i privati che intendono esercitare l'attività di gestore di posta elettronica certificata inviano al CNIPA domanda di iscrizione nell'elenco dei gestori di posta elettronica certificata.
3. I richiedenti l'iscrizione nell'elenco dei gestori di posta elettronica certificata diversi dalle pubbliche amministrazioni devono avere natura giuridica di società di capitali e capitale sociale interamente versato non inferiore a un milione di euro.
4. I gestori di posta elettronica certificata o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione devono, inoltre, possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.
5. Non possono rivestire la carica di rappresentante legale, di componente del consiglio di amministrazione, di componente del collegio sindacale, o di soggetto comunque preposto all'amministrazione del gestore privato coloro i quali sono stati sottoposti a misure di prevenzione, disposte dall'autorità giudiziaria ai sensi della legge 27 dicembre 1956, n. 1423, e della legge 31 maggio 1965, n. 575, e successive modificazioni, ovvero sono stati condannati con sentenza irrevocabile, salvi gli effetti della riabilitazione, alla reclusione non inferiore ad un anno per delitti contro la pubblica amministrazione, in danno di sistemi informatici o telematici, contro la fede pubblica, contro il patrimonio, contro l'economia pubblica, ovvero per un delitto in materia tributaria.
6. Il richiedente deve inoltre:
a. dimostrare l'affidabilità organizzativa e tecnica necessaria per svolgere il servizio di posta elettronica certificata;
b. impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia della posta elettronica e della dimestichezza con procedure di sicurezza appropriate;
c. rispettare le norme del presente regolamento e le regole tecniche di cui

all'articolo 17;
d. applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate;
e. utilizzare per la firma elettronica, di cui all'articolo 9, dispositivi che garantiscono la sicurezza delle informazioni gestite in conformità a criteri riconosciuti in ambito europeo o internazionale;
f. adottare adeguate misure per garantire l'integrità e la sicurezza del servizio di posta elettronica certificata;
g. prevedere servizi di emergenza che assicurano in ogni caso il completamento della trasmissione;
h. fornire, entro i dodici mesi successivi all'iscrizione nell'elenco dei gestori di posta elettronica certificata, dichiarazione di conformità del proprio sistema di qualità alle norme ISO 9000, successive evoluzioni o a norme equivalenti, relativa al processo di erogazione di posta elettronica certificata;
i. fornire copia di una polizza assicurativa di copertura dei rischi dell'attività e dei danni causati a terzi.
7. Trascorsi novanta giorni dalla presentazione, la domanda si considera accolta qualora il CNIPA non abbia comunicato all'interessato il provvedimento di diniego.
8. Il termine di cui al comma 7 può essere interrotto una sola volta esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del CNIPA o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.
9. Il procedimento di iscrizione nell'elenco dei gestori di posta elettronica certificata di cui al presente articolo può essere sospeso nei confronti dei soggetti per i quali risultano pendenti procedimenti penali per delitti in danno di sistemi informatici o telematici.
10. I soggetti di cui al comma 1 forniscono i dati, previsti dalle regole tecniche di cui all'articolo 17, necessari per l'iscrizione nell'elenco dei gestori.
11. Ogni variazione organizzativa o tecnica concernente il gestore ed il servizio di posta elettronica certificata e' comunicata al CNIPA entro il quindicesimo giorno.
12. Il venire meno di uno o più requisiti tra quelli indicati al presente articolo e' causa di cancellazione dall'elenco.
13. Il CNIPA svolge funzioni di vigilanza e controllo sull'attività esercitata dagli iscritti all'elenco di cui al comma 1.

Articolo 15 - Gestori di posta elettronica certificata stabiliti nei Paesi dell'Unione europea

1. Può esercitare il servizio di posta elettronica certificata il gestore del servizio stabilito in altri Stati membri dell'Unione europea che soddisfi, conformemente alla legislazione dello Stato membro di stabilimento, formalità e requisiti equivalenti ai contenuti del presente decreto e operi nel rispetto delle regole tecniche di cui all'articolo 17. E' fatta salva in particolare, la possibilità di avvalersi di gestori stabiliti in altri Stati membri dell'Unione europea che rivestono una forma giuridica equipollente a quella prevista dall'articolo 14, comma 3.
2. Per i gestori di posta elettronica certificata stabiliti in altri Stati membri dell'Unione europea il CNIPA verifica l'equivalenza ai requisiti ed alle formalità di cui al presente decreto e alle regole tecniche di cui all'articolo 17.

Articolo 16 - Disposizioni per le pubbliche amministrazioni

1. Le pubbliche amministrazioni possono svolgere autonomamente l'attività di gestione del servizio di posta elettronica certificata, oppure avvalersi dei servizi offerti da altri gestori pubblici o privati, rispettando le regole tecniche e di sicurezza previste dal presente regolamento.
2. L'utilizzo di caselle di posta elettronica certificata rilasciate a privati da pubbliche amministrazioni incluse nell'elenco di cui all'articolo 14, comma 2, costituisce invio valido ai sensi del presente decreto limitatamente ai rapporti intrattenuti tra le amministrazioni medesime ed i privati cui sono rilasciate le caselle di posta elettronica certificata.
3. Le pubbliche amministrazioni garantiscono ai terzi la libera scelta del gestore di posta elettronica certificata.

4. Le disposizioni di cui al presente regolamento non si applicano all'uso degli strumenti informatici e telematici nel processo civile, nel processo penale, nel processo amministrativo, nel processo tributario e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti, per i quali restano ferme le specifiche disposizioni normative.

Articolo 17 - Regole tecniche

1. Il Ministro per l'innovazione e le tecnologie definisce, ai sensi dell'articolo 8, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sentito il Ministro per la funzione pubblica, le regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata. Qualora le predette regole riguardino la certificazione di sicurezza dei prodotti e dei sistemi e' acquisito il concerto del Ministro delle comunicazioni.

Articolo 18 - Disposizioni finali

1. Le modifiche di cui all'articolo 3 apportate all'articolo 14, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, (Testo A) si intendono riferite anche al decreto del Presidente della Repubblica 28 dicembre 2000, n. 444 (Testo C). Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addi' 11 febbraio 2005

CIAMPI

Berlusconi, Presidente del Consiglio dei Ministri

Baccini, Ministro per la funzione pubblica

Stanca, Ministro per l'innovazione e le tecnologie

Siniscalco, Ministro del-l'economia e delle finanze

Visto, il Guardasigilli: Castelli

Registrato alla Corte dei conti il 18 aprile 2005

Registro n. 4, Ministeri istituzionali, foglio n. 332