CONSIGLIO REGIONALE DEL PIEMONTE

Dossier informativo per i Consiglieri regionali

Informatica e digitalizzazione nella Pubblica Amministrazione

Quattordici

Febbraio 2006

Collana pubblicazioni
Direzione Processo Legislativo

Informatica e digitalizzazione nella Pubblica Amministrazione

Direzione Processo Legislativo
Adriana Garabello

Realizzazione a cura di:
Chiara Casagrande, Federica Moi
Settore Studi e Documentazione Legislativi

Schede tratte dalla banca dati "Archivio giuridico"
Settore Studi e Documentazione Legislativi

Febbraio 2006

INDICE

PRESENTAZIONE

La presente pubblicazione consiste in una raccolta di "schede" tratte dall' "Archivio giuridico", banca dati contenente materiale documentale di natura normativa, giurisprudenziale e dottrinale, aggiornata quotidianamente per la segnalazione delle novità, curata dal settore Studi e documentazione legislativi e in libera consultazione sul sito del Consiglio Regionale (www.consiglioregionale.piemonte.it/LGEXTR/servlet/SErvNOTI),.

Un breve cenno di presentazione dell'archivio giuridico è necessario per comprendere appieno la struttura di questa pubblicazione.

La banca dati costituisce il risultato di una costante attività di ricerca, selezione, studio e comparazione delle informazioni tratte da quotidiani, riviste specializzate (cartacee e on line) e siti web e oggetto di successiva catalogazione e archiviazione.

Le segnalazioni, accompagnate da un commento sintetico ma esaustivo, intendono fornire un servizio di supporto all'attività dei Consiglieri regionali, delle strutture interne al Consiglio e di tutti gli utenti esterni eventualmente interessati.

L'Archivio giuridico è un sistema d'informazione, dotato di una duplice funzionalità, che consente:

- *la consultazione, nella bacheca delle "News", delle segnalazioni giornaliere inerenti le notizie e i commenti più recenti e interessanti;*
- *la ricerca di tutta la documentazione presente nell'Archivio, catalogata sulla base di voci e sottovoci studiate in funzione di un'agile consultazione tematica attraverso classificatori fissi.*

L'Archivio giuridico è stato infatti ordinato prevedendo campi fissi (classificazione dell'argomento trattato ed eventuale sottoclassificazione, fonte da cui l'informazione è stata reperita, autore in caso di commenti, tipo di atto

esaminato, organo emanante e data dell'atto) e una sezione, denominata "abstract", contenente un commento alla notizia segnalata.

Per consentire l'immediata reperibilità dei testi oggetto delle segnalazioni (prevalentemente leggi, regolamenti, atti amministrativi, sentenze, dottrina), questi vengono allegati. Non sono invece posti a corredo delle schede quei documenti la cui riproduzione è riservata; in questi casi la consultazione del materiale è consentita direttamente presso il Settore.

Per quanto attiene alle modalità di ricerca, occorre distinguere fra News e schede di segnalazione.

La pagina iniziale contiene l'elenco delle ultime quaranta notizie inserite (in giornata e nei giorni immediatamente precedenti). Di ogni scheda appare il numero e il relativo titolo, in grado di illustrare in maniera esauriente l'argomento esaminato. La scheda è consultabile cliccando sul numero identificativo.

Le altre schede, riguardanti argomenti di interesse, ma di non stretta attualità, possono essere reperite nell'ambiente di consultazione. Il materiale giuridico, archiviato secondo classificazione specifica, può essere ricercato in modo agevole per materia, organo emanante, parola chiave o attraverso i riferimenti legislativi e giurisprudenziali.

Ai fini della redazione del volume in oggetto sono state selezionate due voci fra le molte comprese nel menù "classificazione: "E-government" e "Informatica".

La scelta di queste materie trova giustificazione nella loro attualità e nella "generalità" delle stesse: la legislazione e la giurisprudenza in materia di e-government e di diritto dell'informatica vengono infatti ad avere riflessi su quasi tutti i settori del diritto.

La voce E-government, alla quale corrisponde la prima parte della pubblicazione, si articola nelle seguenti sottoclassificazioni (che, nella pubblicazione costituiscono i capitoli): "Informatizzazione P.A.", Progetti di e-government" "Firma digitale", "Posta elettronica", "Protocollo Informatico", "Codice dell'amministrazione digitale", mentre la voce "Informatica", che costituisce la seconda parte, si suddivide in "Nomi di dominio", "Processo telematico", "Reati informatici" .

La terza parte è dedicata ai "Rapporti fra privacy e posta elettronica".

All'interno di ciascuna classificazione e sottoclassificazione sono raccolte le schede dell'archivio, dalla più recente a quella di più vecchia data.

Vi è infine una appendice costituita dalla presentazione dei siti principali nelle materie dell'e-government e del diritto dell'informatica.

Il punto di forza della pubblicazione è da ricercare nella sua struttura: non è infatti il tradizionale volume monografico in materia di e-government e di diritto dell'informatica, ma un insieme di schede che illustrano le principali novità in materia: ad un commento sintetico segue, di regola, il testo o se si tratta di articoli dottrinali, vi sono i riferimenti bibliografici e viene segnalata la possibilità di consultare la rivista presso il settore.

In tal modo si auspica che il lettore riesca a rendersi immediatamente conto delle più importanti e più recenti novità nelle materie trattate con la possibilità però, con la lettura delle schede meno recenti, di seguire il percorso che il legislatore (nonché i giudici e la dottrina) hanno seguito nell'ambito delle materie analizzate.

Parte I

PARTE I: E-GOVERNMENT

La materia dell'e-government è stata selezionata in ragione della sua attualità: le tecnologie dell'informazione e delle telecomunicazioni sono, come evidenziato nella relazione annuale 2004 del Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA), presentata a Roma il 5 giugno 2005, uno dei fattori produttivi essenziali.

Nel citato rapporto si specifica che la spesa informatica della pubblica amministrazione è di tre miliardi di euro, di cui un miliardo e settecento milioni riferibili alle amministrazioni centrali ed un miliardo e trecento milioni alle amministrazioni locali.

E-government significa utilizzo delle tecnologie informatiche nella pubblica amministrazione e in tutti i processi amministrativi nonché erogazione di servizi pubblici finalmente capaci di corrispondere in modo più efficace e trasparente alla domanda collettiva di prestazioni efficienti.

Per e-government si intende quindi un amministrazione pubblica on line, che dispone di servizi efficienti, dinamici e moderni, il cui presupposto è un nuovo modo di pensare e di regolare giuridicamente il rapporto tra privati e pubblica amministrazione.

Per i cittadini l'e-government significa, concretamente, la fine di procedure farraginose e di lunghe file e anche non dover più fornire reiterate volte informazioni di cui la pubblica amministrazione è già in possesso.

Per quanto riguarda le imprese, l'amministrazione on line permette di migliorare la competitività riducendo il costo dei pubblici servizi.

L'e-government consente di accrescere la trasparenza, assicurare la parità di accesso ai servizi, rafforzare la partecipazione dei cittadini ai processi democratici e all'elaborazione delle politiche pubbliche.

E-government è quindi anche indice di efficienza della Pubblica Amministrazione e di incremento delle sue capacità di fornire sul territorio informazione, documentazione e servizi a favore di associazioni, categorie, imprese e singoli cittadini.

Come evidenziato nel sito del dipartimento per l'Innovazione e le Tecnologie, il modello che si vuole implementare è quello di una Pubblica Amministrazione orientata all'utente, cittadino ed impresa, fornitrice di moderni servizi, creatrice di valore pubblico, con cui sia facile operare.

Una pubblica amministrazione efficiente e trasparente nei suoi compiti e nel suo grande patrimonio informativo, è anche e soprattutto un fattore di innovazione e di competitività.

Gli interventi normativi attuati a livello di e-government si sono susseguiti rapidamente negli ultimi anni.

Le politiche sull'e-government del Ministro per l'Innovazione e le Tecnologie sono state definite all'interno delle Linee Guida del Governo per lo sviluppo della Società dell'Informazione nella legislatura, pubblicate nel giugno 2002.

In questo documento le iniziative rivolte alle Pubbliche Amministrazioni sono armonizzate a quelle rivolte al sistema paese nel suo complesso, al fine di uno sviluppo coordinato e coerente di tutte le sue componenti.

Le Linee Guida prevedono di conseguire i 10 obiettivi di legislatura fissati dal Comitato dei Ministri per la Società dell'Informazione nel febbraio 2002.

Tali obiettivi riguardano le macro aree della messa on-line dei servizi pubblici, dell'efficienza interna, della valorizzazione delle risorse umane, della trasparenza e della qualità.

Gli obiettivi impegnano in primo luogo le amministrazioni centrali, ma potranno essere di indirizzo anche per le regioni e gli enti locali, che li perseguiranno all'interno delle loro azioni di e-government a livello territoriale.

Il Ministro per l'Innovazione e le Tecnologie ha inoltre fissato gli obiettivi e le linee di intervento per l'anno 2002 con una apposita Direttiva (Linee Guida in materia di digitalizzazione dell'amministrazione per il 2002).

Con direttiva del 20 dicembre 2002 ha poi indicato le priorità da recepirsi nelle direttive dei vari Ministri per l'anno 2003, in coerenza con quanto previsto dalla direttiva del Presidente del Consiglio dei Ministri dell'8 novembre 2002.

Con la direttiva del 18 dicembre 2003 sono state fornite le "Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004". Tale atto di indirizzo individua le priorità di azione per il 2004 proseguendo nella realizzazione del disegno organico di innovazione illustrato nelle Linee Guida del Governo approvate dal Consiglio dei Ministri a maggio 2002 e condiviso con le Autonomie Locali con la sottoscrizione del documento "L'e-government per un federalismo efficiente: una visione condivisa, una realizzazione cooperativa".

Le linee guida per l'anno 2005, pubblicate sulla Gazzetta Ufficiale n. 35 del 12 febbraio 2005, fanno il punto su ciò che si è fatto e ciò che si deve ancora realizzare fornendo alle Amministrazioni obiettivi da raggiungere e direttive sulle modalità d'attuazione.

La prima fase del processo di digitalizzazione della PA ha, infatti, mirato a promuovere le iniziative d'innovazione attraverso il cofinanziamento di progetti sul territorio stimolando la cooperazione e l'interoperabilità tra gli enti e, in generale, la diffusione della "cultura dell'innovazione" che impone di sostituire gli strumenti e le modalità "tradizionali" nel rapporto cittadino-PA e nello svolgimento delle attività interne alla PA stessa.

Gli ultimi importanti interventi normativi in materia sono:

- *il decreto legislativo sul "Sistema Pubblico di Connettività" con l'obiettivo di collegare per via telematica tutte le Amministrazioni pubbliche del Paese*
- *la pubblicazione del "Codice dell'Amministrazione digitale" con l'obiettivo di fornire un assetto unitario ed organico al complesso di diritti dei cittadini e delle imprese e ai doveri delle Amministrazioni in materia di digitalizzazione delle pubbliche amministrazioni.*

Un breve cenno infine alle politiche di e-government nell'ambito della Regione Piemonte[1].

Il Piano di e-government piemontese parte dal presupposto che "la PA deve diventare fornitore di un cliente che si chiama cittadino o impresa. Di conseguenza, occorre progettare infrastrutture e servizi perché il livello di interazione migliori". I temi principali su cui si articola sono pertanto :

- *la definizione dei ruoli;*
- *l'individuazione di obiettivi strategici.*

Con il trasferimento di funzioni e compiti amministrativi dal centro alle periferie, gli Enti territoriali sono infatti chiamati a raggiungere nuovi obiettivi. La Regione, elemento centrale della riforma dello Stato in senso federalista, "è chiamata a svolgere un ruolo di impulso e coordinamento nel ridisegno del sistema delle collettività locali"; "la Provincia, Ente locale intermedio tra Comune e Regione", rappresenta "il riferimento in ambito territoriale di interessi finalizzati alla costruzione, diffusione, gestione e sostegno del nuovo sistema informativo a livello territoriale e svolge un ruolo di back-office e di assistenza agli Enti locali"; i Comuni assumono il ruolo di front-office in quanto "soggetti naturali di governo ed interlocutori primari nei rapporti fra cittadini e PA"; i Comuni e le Comunità Montane, per assolvere al meglio le nuove e più ampie responsabilità, si avvicinano al mondo delle nuove tecnologie in forma associata.

Nello specifico, in Piemonte, l'affermazione del nuovo modello di sviluppo e gestione dei servizi delineato dai principi di e-government è favorita da alcune peculiarità:

- *la frammentazione del numero di Enti locali e la polverizzazione sul territorio come fattori di stimolo per l'efficienza di collegamenti e servizi di rete e per la promozione dell'associazionismo;*
- *la vocazione tecnologica e la progettualità diffusa, condizioni indispensabili per la sperimentazione e la costruzione di infrastrutture e di servizi telematici innovativi;*

[1] Le informazioni sull'e-government nella Regione Piemonte sono state tratte dal sito www.ruparpiemonte.it. Si segnala che nell'appendice, nella quale sono raccolti alcuni siti di particolare rilievo nell'ambito delle materie dell'e-government e dell'informatica, c'è una breve sezione dedicata ai "siti del Piemonte".

- *l'esistenza di Rupar Piemonte, intesa come infrastruttura per l'erogazione di servizi, strumento di cooperazione e luogo di incontro e confronto;*
- *l'organizzazione in rete della PA locale, in raccordo con la PA centrale, grazie anche alla presenza del modello CSI (modello consortile, pubblico, che riesce a promuovere sinergie nella logica della costruzione del Sistema Piemonte per l'attuazione del decentramento attraverso l'uso delle tecnologie dell'informazione);*
- *la presenza della "Conferenza Permanente Regione-Autonomie Locali", quale organo di rappresentanza degli Enti locali piemontesi e tavolo per la concertazione dei processi di delega e di riforma federalista dello Stato;*
- *l'esistenza di consolidati strumenti di lavoro quali i Piani di sviluppo del Sistema Informativo ai vari livelli territoriali.*

I documenti tecnici e legislativi che completano il Piano dettagliano alcuni aspetti dell'e-government piemontese, sottolineando come ogni singolo ente locale possa diventarne parte attiva allo scopo di "realizzare l'interoperabilità telematica, rendere possibile l'erogazione di servizi integrati di sportello ai cittadini e alle imprese rispondenti alla nuova visione e permettere l'accesso telematico alle informazioni e ai servizi di tutte le PA" .

Il testo integrale del Piano di e-government piemontese è disponibile al sito http://www.ruparpiemonte.it/e-gov/dwd/egov_piem.pdf

Il 26 marzo 2003 il Presidente della Regione Piemonte e il Ministro per l'Innovazione e le Tecnologie hanno firmato la Convenzione che sancisce la nascita del "Centro Regionale di Competenza per l'e-government" del Piemonte con lo scopo di fornire supporto dedicato al sistema delle PA locali nell'elaborazione delle politiche di sviluppo territoriale.

L'attività del Centro Regionale di Competenza per l'e-government e la società dell'informazione in Piemonte si articola, come sancito dal Piano delle Attività 2004-2005, secondo l seguenti 5 aree tematiche.

Area 1- Assistenza a politiche e processi di innovazione.

Si rivolge sia alle iniziative promosse e gestite dalla Regione sia alle iniziative che derivano da politiche nazionali di innovazione, concertate con il sistema delle Regioni e Autonomie locali a partire dal piano di e-gov. Il CRC svolge, inoltre, funzioni di supporto

e coordinamento dei progetti co-finanziati dal Ministro per l'Innovazione e le Tecnologie (1° e 2° fase).

Area 2 - Formazione.

L'obiettivo è quello di rispondere alle esigenze del fabbisogno formativo individuato in base ad elementi raccolti durante la 1° fase del progetto CRC. Le attività, erogate sotto forma di percorsi di formazione o seminari, mirano ad accrescere le competenze dei soggetti coinvolti nei processi di innovazione.

Area 3 – Comunicazione.

Le azioni di informazione e comunicazione intendono valorizzare i "prodotti" delle azioni locali, intese come sintesi tra i risultati ottenuti e le metodologie utilizzate, che rappresentano oggi un autentico patrimonio di progetto. Nello sviluppo di questa attività, il CRC Piemonte è in stretta collaborazione con lo staff centrale attraverso l'uso dei tradizionali strumenti di comunicazione, oltre che del sito web dedicato (www.crcitalia.it).

Area 4 – Osservatorio.

L'obiettivo dell'Osservatorio CRC è quello di raccogliere e fornire un' informazione più ricca e precisa sulle dinamiche evolutive dell'e-government e della società dell'informazione a livello locale, nonché sull'utilizzo dei servizi pubblici innovati da parte di cittadini e imprese. Grazie a regole comuni fornisce una visione coerente, comparabile e aggregata a livello nazionale (e, in prospettiva, europea).

Area 5 – Sviluppo tematico.

La necessità di approfondire alcune tematiche oggetto delle attività svolte a supporto delle Amministrazioni locali è sempre stata ben presente tra gli obiettivi dei componenti della rete dei CRC. Nell'ambito dell'incontro dei CRC Bagni di Tivoli (RM) il 12 novembre 2003, si sono individuati i macro temi oggetto di studio, tra i quali open source, e-learning e accessibilità.

Per quanto concerne il Consiglio Regionale del Piemonte, già a partire dal 2003, veniva messo in luce come il nuovo modello di sistema informativo consiliare, orientato a

perseguire obiettivi di E-governance e E-democracy, distingue due macro aree di intervento[2]*:*

1) la prima, che può essere definita a "valenza interna", è imperniata essenzialmente sull'attività di supporto al legislatore nell'esercizio delle sue peculiari competenze, ossia legiferare, controllare e rappresentare. Le prime due, in particolare, sono caratterizzate da forti contenuti decisionali che richiedono idonei strumenti di supporto, in parte già presenti, ma suscettibili di essere rinnovati e arricchiti di altre funzionalità oltre ad essere maggiormente diffusi e più intensamente utilizzati.

2) La seconda, a "valenza esterna", ha come fulcro l'informazione verso la comunità e si deve configurare non come attività di tipo statico e unidirezionale, ma puntare al rapporto dinamico ed interattivo tra istituzioni e società nel suo complesso, ponendo il cittadino "al centro del sistema".

Il patrimonio informativo e di conoscenza dell'ente è l'elemento caratterizzante, la base di partenza che genera e alimenta il dialogo, la partecipazione e la codecisione.

L'ambiente realizzativo comune è costituito dal Sistema Informativo del Consiglio Regionale del Piemonte (SiCR) e dai suoi strumenti attraverso l'utilizzo delle nuove tecnologie e delle reti di comunicazione.

Il Piano di Attività 2005[3] *del SICR illustra i progetti relativi alle attività previste dal Piano 2004-2006 nonché le attività integrative previste dal Piano 2005.*

---

[2] Si cita, qui di seguito, il capitolo concernente "Il nuovo modello di Assemblea digitale", contenuto nelle "Linee del piano di sviluppo 2004-2006", a cura del Sistema informativo del Consiglio Regionale del Piemonte.

[3] Si riporta l'indice.

Fra i molteplici risultati realizzati si cita, per la sua importanza, il completamento e la messa a regime della versione definitiva del Dossier virtuale delle leggi e dei progetti di legge (consultabile al seguente indirizzo: www.consiglioregionale.piemonte.it/dvpdlint/jsp/Start.jsp).

Si evidenzia, infine, che sul Bollettino Ufficiale n. 5 del 2 febbraio 2006 è stata pubblicata la legge regionale n. 4 del 30 gennaio 2006 "Sistema regionale per la ricerca e l'innovazione".

Con questa legge, che consta di diciassette articoli, la Regione Piemonte "nell'esercizio della propria potestà legislativa concorrente in materia di ricerca scientifica e tecnologica e sostegno all'innovazione per i settori produttivi prevista dall'articolo 117 della Costituzione, organizza, promuove e coordina il sistema regionale della ricerca all'interno dello Spazio europeo della ricerca".

Si segnala, in particolare, la previsione dell'istituzione del Comitato regionale per la ricerca e l'innovazione, di una Commissione scientifica e del Coordinamento tecnico regionale per la ricerca e l'innovazione.

Come anticipato nell'introduzione, la prima parte della pubblicazione, relativa all'e-government, si articola nelle seguenti sezioni, ciascuna dedicata ad un particolare settore dell' "amministrazione digitale" :

- *"Informatizzazione P.A."*
- *"Progetti di e-government".*
- *"Firma digitale"*
- *"Posta elettronica"*
- *"Protocollo Informatico"*
- *"Codice dell'amministrazione digitale"*

CAPITOLO I

INFORMATIZZAZIONE P.A.

Le pubbliche amministrazioni hanno assistito, in questi ultimi anni, alla continua e rapida evoluzione delle tecnologie dell'informazione e della comunicazione, le quali costituiscono un importante strumento di innovazione, capace di incidere sulle attività e sui comportamenti degli individui e delle imprese, nonché sugli eventi sociali ed economici della società stessa. Questa evoluzione ha comportato l'accentuarsi dell'attenzione dei governi per l'Information Technology (IT) e per la sua valenza strategica come fattore di ammodernamento delle strutture pubbliche. Le tecnologie dell'informazione e della comunicazione sono infatti strumento chiave per la trasformazione e l'integrazione delle amministrazioni degli stati dell'Unione Europea, in quanto fattore abilitante del cambiamento. Il tema dell'IT ha assunto una rilevanza tale da indurre tali Paesi a predisporre dei mezzi di definizione e di armonizzazione delle politiche di innovazione tecnologica, nonché ad investire enti appositamente istituiti, ovvero direttamente organi di Governo, della responsabilità in ordine alla promozione ed allo sviluppo dell'informatica pubblica nel territorio di competenza. L'esigenza di assicurare all'IT della pubblica amministrazione uno sviluppo ordinato in termini istituzionali si è manifestata sin dalla prima metà degli anni novanta, quando, nel 1993, è stato istituito un apposito organismo centrale, con il rango di Autorità, che, possedendo capacità di indirizzo tecnico-organizzativo, aveva la funzione di coordinare e pianificare le iniziative e gli investimenti statali nell'ambito del generale processo di informatizzazione delle pubbliche amministrazioni, al fine di garantire la razionale utilizzazione e l'interconnessione dei sistemi informatici delle amministrazioni.

Negli anni Novanta, il ruolo esercitato dai suddetti sistemi informativi è andato sempre più modificandosi: essi, infatti, da mero strumento di ausilio per le singole amministrazioni pubbliche, si sono trasformati in vere e proprie strutture informative

decentrate di settore, poste al servizio di una pluralità di utenti, a livello centrale e locale, coinvolti nelle varie politiche. In questo scenario, si è radicata, anche in Italia, la convinzione che il governo dell'IT pubblica costituisce un importante strumento di sviluppo non solo per la pubblica amministrazione, ma anche per l'economia dell'intera società. Gli indirizzi strategici dei documenti di programmazione economica e finanziaria e le direttive del Ministro per l'innovazione e le tecnologie, hanno dato grande importanza allo sviluppo del cosiddetto governo elettronico attraverso:

- la progettazione di servizi on-line, sia accedendo ad applicazioni esistenti che a nuove applicazioni che integrino i dati di diverse amministrazioni;

- l'analisi della capacità delle organizzazioni pubbliche a imbarcarsi in un piano di trasformazione basato sulle tecnologie informatiche;

- la definizione dei criteri di interoperabilità tra le amministrazioni;

- la creazione delle strutture di governo e di indirizzo strategico;

- le modalità di comunicazione e coinvolgimento degli utenti (cittadini, imprese, terzo settore, etc.).

Tale strumento, infatti, essendo un complemento naturale dello sviluppo della Società dell'Informazione, contribuisce al miglioramento del livello dei servizi: si pensi, ad esempio, alle piccole e medie imprese che potranno interagire con le amministrazioni in maniera elettronica per ottemperare agli obblighi di legge ovvero richiedere documentazione e ottenere informazioni.

In questo quadro il ruolo del Dipartimento della funzione pubblica è orientato a migliorare la capacità delle amministrazioni nel cogliere le opportunità offerte dalle tecnologie, tenendo conto di due delicati equilibri: quello tra innovazione tecnologica e innovazione organizzativa e- quello tra canali innovativi e tradizionali di erogazione dei servizi.

Per quanto concerne la Regione Piemonte[4] *è ormai da anni in corso un'intensa politica di innovazione e di promozione delle ICT (Information and Communication*

[4] Le informazioni sull'informatizzazione nella Regione Piemonte sono state tratte dal sito www.ruparpiemonte.it

Technologies), che ha dato una spinta decisiva alla trasformazione del tessuto economico e sociale regionale da società industriale a società dell'informazione e del terziario.

In tal senso le Amministrazioni regionali hanno messo in campo alcuni dei loro punti di forza, tra cui un'elevata competitività tecnologica, la presenza di imprese a dimensione internazionale, un sistema formativo all'avanguardia e con buona copertura territoriale, una competitività manifatturiera con orientamento alla concertazione e un alto potenziale culturale. L'attenzione per lo sviluppo della Società dell'Informazione, insomma, ha costituito uno degli aspetti del più generale progetto di "innovazione" regionale. Un progetto facilitato anche dall'azione di riforma e di ammodernamento tecnologico della Pubblica Amministrazione regionale portata avanti dal CSI-Piemonte (www.csi.it), il Consorzio per il Sistema Informativo che da oltre 25 anni contribuisce alla crescita tecnologica del territorio piemontese.

La visione che sottintende le politiche e le iniziative legate all'e-government e alla promozione della Società dell'Informazione è quella del "Sistema Piemonte", a cui partecipano, oltre alle PA, le varie componenti dell'economia regionale. Quello del "Sistema Piemonte" è un modello organizzativo che vede la PA piemontese innovarsi attraverso progetti di investimento realizzati con la partecipazione di tutti gli Enti locali, chiamati a rispondere in modo veloce ed efficace alle richieste di cittadini e imprese. Lavorare in una logica sistemica significa promuovere strategie cooperative, realizzare progetti inter-ente, produrre economie di scala. Il risultato di tali interventi consiste nello sviluppo di soluzioni condivisibili e riusabili da tutti gli Enti, in grado di semplificare l'azione amministrativa locale, con una duplice ricaduta: aumentare l'efficienza operativa degli Enti e migliorare la qualità dei servizi resi agli utenti della PA.

Storicamente uno dei maggiori risultati piemontesi è stato, nel 1997, la realizzazione di un'infrastruttura di rete regionale denominata "PiemonteinRete". Realizzata nel rispetto delle linee guida fissate dall' Autorità per l'informatica nella pubblica amministrazione (AIPA)[5], "PiemonteinRete" è partita dalle reti esistenti di

[5] In attuazione di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato sul supplemento ordinario n. 123 alla Gazzetta Ufficiale n. 174 del 29 luglio 2003, l'Autorità per l'informatica nella pubblica amministrazione è stata trasformata in Centro nazionale per l'informatica nella pubblica amministrazione.

settori quali Sanità, Agricoltura e Biblioteche e ha permesso il collegamento di tutti gli uffici regionali con gli altri Enti presenti sul territorio.

"PiemonteinRete" contemplava fin dalle origini l'integrazione nella Rete Unitaria della Pubblica Amministrazione. Tale integrazione è avvenuta nel 1999 con la transizione a RuparPiemonte, la Rete Unitaria della Pubblica Amministrazione Regionale (www.ruparpiemonte.it) che raccoglie oggi oltre 2.250 Enti locali piemontesi (fra cui tutti i 1.206 Comuni).

Uno strumento importantissimo di policy e di programmazione regionale è stato il Piano di e-government piemontese, elaborato sulla base di quanto previsto nel Piano nazionale e approvato, nelle sue linee guida, dalla Conferenza Permanente Regione-Autonomie Locali l'11 aprile 2001.

Il Piano riflette la progettualità diffusa delle PA piemontesi, che si manifesta negli investimenti nel settore ICT promossi dai singoli Enti. Strumento di azione prioritario del "Sistema Piemonte" è la già citata RuparPiemonte, da sempre concepita come un sistema informativo unitario e integrato in cui far confluire le risorse provenienti non solo dalla PA ma anche dal comparto produttivo e socioculturale. Un'infrastruttura che non è quindi da intendersi come semplice rete di trasporto dati, ma come occasione di partecipazione, formazione, condivisione, attuazione e consolidamento di progetti che fanno della regione un sistema unitario.

Le principali linee di azione individuate dal piano riguardano:

- la realizzazione di interventi infrastrutturali, attraverso il potenziamento della RUPAR e delle tecnologie di trasporto e interconnessione; la sperimentazione di servizi di sicurezza applicativa e di servizi di accesso per cittadini e imprese; l'utilizzo dei servizi esistenti per il reciproco accesso tra Sistemi Informativi di PA diverse;

- il miglioramento della circolazione dei dati pubblici attraverso lo sviluppo di banche dati condivise e di servizi di interoperabilità;

- lo sviluppo di servizi on line per cittadini e imprese e l'interscambio informativo con le imprese, in particolare nel comparto del lavoro;

- la creazione di portali per semplificare il dialogo tra Amministrazioni, con la costituzione di un Centro Servizi per il collegamento di tutti i Comuni;

- la connessione in rete di tutte le scuole, la formazione professionale, la messa in comune di esperienze di didattica e l'accesso a musei virtuali;

- gli investimenti a favore della Montagna, con iniziative che coinvolgono le Comunità Montane e le regioni confinanti, per collegare e valorizzare il territorio montano;

- la promozione dell'open source quale strumento strategico delle PA, volano di sviluppo e opportunità per le imprese del territorio.

Pubblicata sulla Gazzetta Ufficiale la direttiva sulla qualità dei servizi *on line.*

NUMERO SCHEDA: 6704

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: GAZZETTA UFFICIALE

NUMERO: 243

DATA: 18/10/2005

NATURA ATTO: DIRETTIVA

DATA ATTO: 27/07/2005

ORGANO: MINISTERI

Sulla Gazzetta Ufficiale n. 243 del 18 ottobre 2005 è stata pubblicata la direttiva 27 luglio 2005 della presidenza del Consiglio dei ministri, Dipartimento per l'Innovazione e le Tecnologie, avente ad oggetto "*Qualità dei servizi on line e misurazione della soddisfazione degli utenti*".
Obiettivo della direttiva è fornire indicazioni per migliorare la qualità e promuovere l'utilizzo dei servizi-on line, attraverso un'attenta ed efficace rilevazione delle esigenze e delle aspettative degli utenti.
Il Cnipa fornirà supporto informativo, di consulenza e di indirizzo. Supporterà inoltre le amministrazioni nell'individuazione delle criticità da superare, fornirà indicazioni per verificare completezza, usabilità dei servizi erogati on line e nel ricercare le soluzioni più idonee a risolvere problemi tecnici ed organizzativi.

Si allega il testo della direttiva.

PRESIDENZA DEL CONSIGLIO DEI MINISTRI DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE

DIRETTIVA 27 luglio 2005
Qualita' dei servizi on-line e misurazione della soddisfazione degli utenti.
IL MINISTRO
PER L'INNOVAZIONE E LE TECNOLOGIE
di concerto con
IL MINISTRO PER LA FUNZIONE PUBBLICA

E m a n a

la seguente direttiva per la qualita' dei servizi on-line e la misurazione della soddisfazione degli utenti.

Obiettivi della direttiva.

1. Obiettivo della presente direttiva e' fornire indicazioni per migliorare la qualita' e promuovere l'utilizzo dei servizi on-line, attraverso un'attenta ed efficace rilevazione delle esigenze e delle aspettative degli utenti. In particolare vengono forniti indirizzi e linee guida per: a) perseguire maggiore efficacia e tempestiva rispondenza alle aspettative degli utenti attraverso l'utilizzo della rete e le tecnologie informatiche, sia per progettare nuove modalita' di interazione non condizionate da vincoli temporali e logistici, guidate da un'informazione mirata e agevolmente fruibile, esaustiva nel conseguimento del risultato atteso, sia per rilevare il gradimento degli utenti facendo emergere i bisogni reali; b) promuovere l'utilizzo delle tecnologie per realizzare servizi on-line che consentano all'utente di accedere al servizio indipendentemente dal canale utilizzato e all'amministrazione di non dover duplicare informazioni e dati relativi al servizio e al richiedente; cio' al fine di semplificare i rapporti P.A. - cittadini ed imprese; c) incentivare la fruizione dei servizi on-line, in modo da soddisfare le diverse tipologie di utenti, offrendo loro una piu' ampia scelta, ed attenuare la pressione sui canali di erogazione tradizionali consentendo di ridurre i costi di front-office. 2. Scenario di riferimento. Nel continuo processo di trasformazione e modernizzazione delle amministrazioni pubbliche, hanno assunto particolare importanza il tema della qualita' dei servizi pubblici e il ruolo centrale del cittadino, non solo come destinatario di servizi, ma anche quale risorsa strategica da coinvolgere per valutare la rispondenza dei servizi erogati ai bisogni reali (si veda la direttiva del Ministro per la funzione pubblica in data 24 marzo 2004, recante «Misure finalizzate al miglioramento del benessere organizzativo nelle pubbliche amministrazioni»). L'accessibilita' dei servizi e' uno degli elementi piu' qualificanti dell'orientamento al cittadino: Internet, per la sua intrinseca proprieta' di interazione tempestiva e flessibile, rappresenta il canale piu' idoneo ad estenderne la fruibilita'. L'importanza centrale, anche in termini di efficienza, tempestivita' ed economicita', dell'accesso on-line ai servizi delle pubbliche amministrazioni attraverso il canale telematico e' stato peraltro affermato in modo chiarissimo nel «Codice dell'amministrazione digitale» (decreto legislativo 7 marzo 2005, n. 82). Tuttavia, il divario digitale, che e' ancora fortemente presente in alcune fasce della popolazione, comporta la necessita' di un approccio multicanale, per rendere fruibili i servizi sia dal tradizionale sportello sia da canali a cui e' possibile accedere in modalita' remota. Dopo una prima fase di investimenti, stimolati anche da progetti sperimentali e finalizzati, i tempi sono maturi per adottare in modo diffuso il canale di erogazione on-line come componente essenziale di una strategia delle amministrazioni pubbliche improntata alla multicanalita'. Pertanto e' opportuno che le amministrazioni, allorche' introducono o potenziano servizi on-line, riprogettino sostanzialmente la propria offerta in modo da gestire la multicanalita' con criteri razionali. Inoltre deve essere garantita una coerenza complessiva tra le diverse modalita' di erogazione del servizio per evitare disomogeneita' tra i livelli qualitativi nei vari canali. Solo tale strategia, che deve fondarsi su un approccio sistematico, organico e pragmatico, sara' in grado di generare un elevato valore aggiunto per i cittadini, le imprese, le famiglie e gli altri corpi intermedi della societa'. Tale valore puo' essere considerato dal punto di vista: a) economico, in quanto contribuisce ad aumentare la competitivita' dei sistemi locali e del sistema Paese, specialmente per i servizi alle imprese e in genere per le attivita' produttive; b) sociale, in termini di migliore qualita' di vita degli individui e delle comunita'. Nel contesto di una strategia multicanale, l'erogazione dei servizi on-line consente di far emergere la domanda latente in alcuni settori e di rispondere ai nuovi bisogni reali; essa permette inoltre di spostare parte della domanda su una modalita' piu' rapida e maggiormente personalizzata. Inoltre, le moderne tecnologie a supporto dei servizi on-line consentono anche di raccogliere ed elaborare un ingente volume di dati e informazioni dai quali trarre conoscenze sulle tipologie dei bisogni, sui segmenti di utenza, su eventuali barriere culturali e sociali all'utilizzo dei servizi. Tali informazioni, integrate con quelle provenienti dagli altri canali di erogazione, consentono di ridurre, o addirittura eliminare, il rischio di autoreferenzialita' nell'azione delle pubbliche amministrazioni. 3. Classificazione dei servizi on-line e approccio multicanale. Rientrano nell'accezione piu' ampia di «servizi on-line» i servizi non mediati da sportello a cui e' possibile accedere in modalita' remota tramite i seguenti canali: web, chioschi telematici, tv digitale, cali center, telefoni cellulari. La scelta dei canali on-line di erogazione di uno specifico servizio deve essere effettuata tenendo conto sia del livello di interazione necessario alla

sua completa erogazione, sia dei dati che occorre scambiare con l'utente, sia delle specifiche esigenze di fruizione. In relazione alle modalita' di interazione, come affermato nella relazione della Presidenza del Consiglio europeo di Nizza del novembre 2000, i servizi on-line sono classificati dall'Unione europea su quattro livelli, che vanno dalla disponibilita' on-line di informazioni alla possibilita' di scaricare la modulistica, alla possibilita' di attivare un procedimento, allo svolgimento dell'intera transazione on-line. Riguardo ai dati da scambiare, si va da ridotti contenuti non legati allo specifico utente, ad informazioni ponderose e complesse, fino ai dati che permettono un riconoscimento sicuro dell'utente o che forniscono una certificazione della transazione effettuata. In merito alle diverse esigenze di fruizione legate alla tipologia di servizio, occorre valutare se si fruisce del servizio in maniera estemporanea e fortemente delocalizzata (es. info viabilita', pagamento parcheggi, emergenze), ovvero se vi si accede prevalentemente da casa o dall'ufficio. I vari canali disponibili hanno intrinsecamente caratteristiche fortemente diversificate e quindi presentano diversi punti di forza o di debolezza rispetto al peso che i predetti parametri hanno nel singolo servizio. Pertanto, la scelta del canale o dei canali on-line piu' indicati per l'erogazione di un particolare servizio deve essere il risultato di un'attenta mediazione fra i punti di forza dello specifico canale e le caratteristiche salienti del servizio considerato. Al momento, il canale piu' utilizzato per l'erogazione di servizi istituzionali e' il web, stante l'ampiezza e la maturita' delle tecnologie disponibili; comunque, qualunque sia il canale on-line individuato, i criteri generali di approccio ad un risultato di qualita' sono universalmente validi e rimane centrale l'importanza di rilevare la percezione ed i comportamenti dell'utenza. 4. Fattibilita', priorita' e fattori critici di successo. Fattore critico e trainante e' la capacita' di generare un reale e percepibile valore aggiunto per importanti segmenti di utilizzatori dei servizi pubblici. Pertanto e' auspicabile partire da quei servizi che per loro natura e per tipologia di destinatari hanno una maggiore visibilita' e un maggiore impatto sulla soddisfazione degli utenti. Un'elevata qualita' ed efficacia di questi servizi determineranno un effetto di «emulazione», ossia l'aumento della richiesta di erogazione on-line di ulteriori servizi. Per massimizzare la certezza del risultato e' necessario: a) predisporre un piano realistico e fattibile di sviluppo dei servizi on-line, in modo da evitare di generare attese negli utenti eccessivamente elevate rispetto alla capacita' di risposta; b) stabilire un chiaro ordine di priorita' relativo ai servizi da erogare, verificando nell'ottica degli utenti le motivazioni a supporto delle priorita' individuate, e predisporre un piano di sviluppo «integrato», che tenga anche presente l'eventuale necessita' di attivare on-line altri servizi complementari, in mancanza dei quali il valore aggiunto sarebbe limitato; c) perseguire la collaborazione tra amministrazioni per la ricerca di soluzioni replicate o replicabili e per la progressiva eliminazione delle duplicazioni di informazioni, sia in fase di richiesta sia in sede di memorizzazione, attraverso un sempre maggiore utilizzo di processi di cooperazione telematica; d) garantire un'omogenea e costante erogazione dei servizi attraverso i vari canali, in modo tale da soddisfare le diverse tipologie di utenza e valutare nel tempo l'evoluzione della domanda fra i diversi canali; e) valutare i risparmi attesi nel breve e medio periodo dall'offerta dei servizi on-line, confrontandola con i costi di realizzazione e gestione dei nuovi canali, e predisporre una concreta azione di monitoraggio del conseguimento di tali risparmi; f) verificare l'eventuale presenza di impedimenti organizzativi e normativi per l'erogazione dei servizi attraverso i nuovi canali, ed attivare tempestivamente le conseguenti iniziative; g) pianificare un'adeguata azione di informazione e promozione dell'utilizzo del nuovo canale. In tale contesto, qualora le amministrazioni, nella programmazione degli interventi di digitalizzazione dei propri servizi, ravvedano la necessita' o l'opportunita' di semplificare i procedimenti amministrativi e le regolamentazioni interne, ne informano il Dipartimento della funzione pubblica e il Dipartimento per l'innovazione e le tecnologie. 5. La qualita' dei siti e dei portali. L'adozione di una strategia di erogazione dei servizi volta ad estendere la fruizione attraverso il canale web impone alle amministrazioni una particolare attenzione nella progettazione dei siti e dei portali; essi, infatti, vengono a configurarsi come «sportelli virtuali», e cioe' punto di accoglienza e di accesso per un bacino di utenza potenzialmente, ed auspicabilmente, molto piu' esteso e diversificato di quello di qualunque sportello tradizionale. Il loro livello di gradimento, se positivo, rappresenta la condizione necessaria affinche' l'interesse degli utenti di internet si trasferisca sui servizi da essi indirizzati e conseguentemente si concretizzino i positivi ritorni pianificati. Fermo restando quanto previsto in materia di accessibilita' dai provvedimenti di attuazione della legge n. 4 del 2004, di seguito viene indicato un elenco minimo di caratteristiche da considerare per assicurare la qualita' dei servizi offerti da un portale ai suoi utenti: a) accesso ai servizi strutturato

secondo il punto di vista dei segmenti di utenza ai quali si rivolgono; b) percorsi brevi, omogenei e facilmente individuabili; c) presenza di una mappa del sito chiara e sempre aggiornata; d) disponibilita' di funzioni di ricerca semplici ed efficaci; e) aggregazione organica e coerente di informazioni e servizi, correlati fra loro per tematica o finalita', con la possibilita' di accesso diretto dall'uno all'altro. Poiche' e' impossibile, per quanto si vogliano prevedere i bisogni dell'utenza, cogliere a priori ogni tipo di esigenza, e' necessario che nel portale vengano previsti, e chiaramente evidenziati, spazi per il contatto diretto attraverso indirizzi di posta elettronica o numeri verdi. Nell'allegato n. 1 vengono approfonditi gli aspetti tecnico-organizzativi legati all'interazione diretta con gli utenti. 6. La qualita' dei servizi on-line. Per quanto riguarda i servizi informativi on-line, che al momento costituiscono la parte preponderante dell'offerta, occorre che l'informazione resa sia: a) referenziata; b) completa; c) strutturata; d) comprensibile; e) aggiornata; f) uniforme su tutti i canali. Pertanto e' opportuno: a) evidenziare chiaramente l'identita' del soggetto pubblico responsabile dell'informazione, in quanto, stante l'istituzionalita' del servizio, va garantita la fonte e la correttezza dei contenuti; a tal fine, nel caso di servizi erogati attraverso web, si richiama l'importanza dell'utilizzo del dominio «.gov.it», e del rispetto delle procedure per l'acquisizione ed il mantenimento del dominio medesimo, disponibili sul sito del CNIPA; b) per i servizi on-line disponibili su web, creare percorsi di navigazione sufficientemente brevi, anche per l'accesso a documenti ponderosi e complessi, e prevedere link, immediatamente attivabili, ad atti presupposti o correlati; c) introdurre «abstract» che evidenzino chiaramente, e con linguaggio di uso comune, le finalita' e gli ambiti di applicazione dei documenti pubblicati; d) attivare adeguate procedure organizzative che assicurino la tempestiva comunicazione di eventuali modifiche da parte degli uffici competenti; e) in un approccio multicanale, non duplicare i dati relativi ad uno stesso servizio e le relative piattaforme utilizzate (prevedendo invece un unico database per la gestione delle informazioni), in modo da garantire sia alla pubblica amministrazione che all'utente la possibilita' di accedere alle stesse informazioni a prescindere dal canale utilizzato. Per quanto riguarda i servizi transazionali on-line e' opportuno: a) che il servizio sia autoconsistente; di regola, non deve essere richiesto all'utente di utilizzare un altro canale, ed in particolare quello tradizionale dello sportello, al fine di completare il processo. Cio' non toglie che, ove risulti necessario od opportuno, per l'esecuzione delle diverse fasi del servizio si possano utilizzare i diversi canali disponibili e che quindi alcune fasi del processo possano essere svolte con il ricorso ad altri strumenti di comunicazione a distanza di uso comune (es. il fax o la posta); b) che il servizio sia facilmente fruibile; deve essere messa a disposizione una guida all'utilizzo semplice e chiara, fornendo collegamenti immediati a contenuti normativi o informativi correlati, deve essere attivato un recapito telefonico o di posta elettronica per la richiesta di chiarimenti e in tutti i messaggi rivolti all'utente si deve utilizzare un linguaggio che non sia per gli «addetti ai lavori»; c) che per ogni servizio siano pubblicate organicamente e mantenute aggiornate le domande piu' frequenti poste dagli utenti; d) che il servizio realizzi una reale semplificazione delle attivita' che gli utenti devono svolgere, promuovendo, per quanto possibile, l'integrazione in un'unica transazione di piu' adempimenti di competenza di diversi soggetti istituzionali, ma finalizzati al conseguimento di un risultato unitario per l'utente; e) che il servizio offra vantaggi concreti e immediatamente percepibili, quali costi inferiori a quelli richiesti nel caso di utilizzo del tradizionale canale di sportello, scadenze piu' dilazionate, fruibilita' indipendente dagli orari di ufficio; f) che il servizio sia fruibile da tutti; fermo restando, anche in questo ambito, quanto previsto nella gia' citata normativa in materia di accessibilita', e' opportuno che si tenga conto delle esigenze degli stranieri o dei cittadini italiani di origine estera, sia nella predisposizione della modulistica, sia nel prevedere, almeno per i servizi di uso piu' frequente da parte di questa classe di utenti, l'utilizzo delle lingue piu' diffuse; g) che il servizio sia trasparente; e' necessario fornire adeguata informazione sulle caratteristiche e finalita' della transazione ed evidenziare con chiarezza i risultati e gli effetti della transazione una volta attivata, indicare gli eventuali tempi di completamento del processo e delle eventuali ulteriori interazioni necessarie, nonche' consentire di conoscere lo stato di avanzamento dell'iter; h) che l'utente abbia la certezza dell'esito della transazione; sia che il procedimento si concluda in tempo reale, sia che si completi in tempi differiti rispetto alla sua attivazione, all'utente deve essere fornita un'attestazione, equivalente a tutti gli effetti a quella fornita allo sportello, atta ad evidenziare i tempi e le modalita' con le quali ha richiesto il servizio e gli esiti del procedimento. 7. La valutazione della soddisfazione degli utenti. L'attento e continuo monitoraggio del gradimento e delle aspettative dei diversi segmenti di utenze interessati alle varie aree di servizio acquisisce una particolare valenza

nell'erogazione on-line dei servizi stessi, mancando su questo tipo di canale la percezione dell'atteggiamento degli utenti rilevabile nell'ambito del rapporto diretto; pertanto, tale monitoraggio rappresenta un elemento essenziale ed ineludibile dei piani di attivazione dei nuovi canali di erogazione. Per rilevare il gradimento dei cittadini, delle famiglie, delle imprese e degli altri utilizzatori dei servizi e' quindi opportuno gestire in maniera organica tre modalita' tra loro diverse ma i cui risultati vanno integrati: a) una modalita' diretta, attuata attraverso un questionario su web o per via telefonica, da proporre periodicamente; b) una modalita' indiretta fondata sulle informazioni acquisite attraverso le e-mail ricevute, il contact center e ogni altra forma di contatto prevista con gli utenti; c) una modalita' «tecnica» basata sull'analisi dei comportamenti di navigazione. Nell'allegato n. 2 sono forniti dettagli sulle diverse modalita' di rilevazione della soddisfazione degli utenti. La sintesi delle diverse fonti consente una visione piu' articolata e quindi valutazioni piu' complete. In particolare, partendo dai dati «tecnici», possono essere effettuate analisi comportamentali che fanno emergere eventuali punti di forza e di debolezza dei portali. Ad esempio, nel caso del web, interpretando i comportamenti dei navigatori, si possono individuare pagine o sezioni con elevato numero di abbandoni, che evidentemente testimoniano difficolta' nell'attivare le funzionalita' del portale o incompletezza o scarsa capacita' di istradamento; in altri casi il limitato numero di accessi di una sezione rispetto alle altre puo' indicare che l'argomento non e' di interesse per il tipo di utenti di quel portale o che lo stesso e' affrontato in maniera non soddisfacente. Analogamente vanno anche considerati i dati delle e-mail e del contact center perche', ad esempio, un elevato numero di richieste sullo stesso argomento puo' indurre a pensare che probabilmente le indicazioni presenti in materia sul portale sono insufficienti o sono poco chiare. E' opportuno che l'analisi dei comportamenti, delle aspettative e del gradimento degli utenti per i servizi on-line venga condotta anche attraverso la comparazione delle valutazioni effettuate per i singoli canali, sia per individuare e rimuovere criticita' indipendenti dal canale di erogazione, sia per monitorare l'effettivo ritorno degli investimenti sui diversi canali. Cosi', ad esempio, l'alta frequentazione di particolari sezioni di un sito, se non si accompagnasse ad una diminuzione del numero dei contatti, per le stesse sezioni, sugli altri canali, sarebbe un indicatore indiretto di come un'informazione o un servizio sia in generale poco chiara o non coerente, inducendo quindi l'utente a piu' verifiche sui vari canali su cui l'informazione o il servizio vengono erogati. Nel loro complesso, le informazioni rilevate devono configurarsi come l'elemento portante di una strategia evolutiva di successo, per la definizione delle azioni conseguenti e delle relative pianificazioni. E' necessario pertanto: a) predisporre adeguati sistemi e metodologie di analisi che permettano di monitorare il gradimento del servizio offerto, le eventuali richieste di ulteriori servizi o l'ampliamento di quelli esistenti e lo spostamento della domanda tra i vari canali utilizzabili per uno stesso servizio; a tal fine ogni amministrazione puo' utilizzare, nella propria autonomia e responsabilita', gli strumenti che ritiene piu' opportuni, quali questionari on-line, possibilmente collegati anche alla fruizione di specifici servizi, indagini via e-mail, indagini telefoniche guidate attraverso call center, ecc.; b) utilizzare almeno una struttura minima di rilevazione del livello di utilizzo dei servizi sia per quelli di informazione sia quelli transazionali; tale struttura minima di rilevazione e' pubblicata e periodicamente aggiornata sul sito del Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) www. cnipa.gov. it c) partendo dai dati quantitativi, effettuare analisi che facciano emergere ed interpretino i comportamenti dei navigatori per dedurne indicazioni altrimenti non acquisibili; d) integrare quanto rilevato tramite i questionari ad hoc con i dati acquisiti attraverso il contact center, le e-mail e i reclami, che offrono il vantaggio di poter effettuare un monitoraggio continuo delle reazioni spontanee e non condizionate, rispetto alle campagne periodiche di rilevazione del gradimento degli utenti; e) pianificare ed attuare una effettiva circolarita' delle informazioni, in modo che i risultati delle rilevazioni vengano diffusi all'interno dell'organizzazione e in particolare ai responsabili dei singoli processi sia amministrativi sia tecnologici, per le opportune valutazioni e la definizione delle eventuali iniziative necessarie; f) monitorare periodicamente l'effettiva attivazione delle azioni conseguenti. I sistemi di rilevazione devono essere attivati entro sei mesi dall'emanazione della presente direttiva. 8. La funzione di supporto. Presso il CNIPA e' istituito un centro di competenza a disposizione delle amministrazioni per l'attivazione degli adempimenti previsti dalla presente direttiva. Il centro fornisce supporto informativo, di consulenza diretta e di indirizzo finalizzato ad assicurare: a) la messa a fattor comune di conoscenze ed esperienze tecnologiche e organizzative; b) una maggiore efficacia degli interventi, in termini di consulenza e di assistenza alle pubbliche amministrazioni; c) la diffusione delle conoscenze relative a

progetti nazionali o internazionali con obiettivi simili. Per le amministrazioni che non ritengono di poter attivare autonomamente la rilevazione diretta del gradimento degli utenti, a richiesta delle stesse puo' essere realizzato, a cura del CNIPA, un ambiente di pubblicazione di questionari on-line in cui la singola amministrazione abbia uno spazio standard dedicato, collegabile dal proprio sito, nonche' servizi per l'elaborazione e la prospettazione dei dati. La decisione in merito all'attivazione di tale servizio e' assunta in funzione del numero di adesioni ad un protocollo di intesa che sara' reso disponibile sul sito CNIPA, contenente le caratteristiche generali del servizio proposto. Il CNIPA inoltre supporta le amministrazioni nell'individuazione delle criticita' da superare per un'efficace erogazione on-line dei propri servizi, collaborando a verificarne la completezza e la usabilita' nella prospettiva degli utenti finali, nonche' a ricercare le soluzioni piu' idonee a risolvere eventuali problemi tecnici o organizzativi.

Allegato n. 1
La qualita' dei siti e dei portali.
Aspetti tecnici e organizzativi dell'interazione con l'utente

Nell'erogazione dei servizi on-line l'interazione con l'utente attraverso il contatto diretto rappresenta una componente essenziale per l'efficacia del servizio stesso, da attuarsi almeno per mezzo del canale telefonico (contact center) e della posta elettronica. In particolare, per quanto riguarda il contact center, gli operatori devono avere una formazione adeguata a comprendere il problema dell'utente, guidarlo, se necessario, a definire con chiarezza il proprio quesito, e a dare comunque una risposta circostanziata ancorche' interlocutoria (ad esempio, chiarire a chi viene inoltrato il quesito, modalita' e tempi stimati per la risposta); inoltre devono disporre di un'adeguata infrastruttura tecnico-organizzativa per tracciare l'interazione in maniera strutturata, inoltrarla correttamente e tempestivamente e monitorarne gli esiti. Analogamente, per quanto riguarda l'interazione per posta elettronica e' opportuno che l'utente venga guidato, nello strutturare il proprio quesito, suggerimento o reclamo, in maniera da individuare facilmente l'ufficio competente, agevolare la risposta, tracciare in maniera omogenea e organica l'interazione; ad esempio, e' utile impostare la e-mail prevedendo dei campi predefiniti che individuino il tipo di messaggio e l'argomento relativo, possibilmente estratto da una lista di parole chiave da selezionare. Infine, e' necessario predisporre adeguate procedure organizzative che assicurino la tempestiva e puntuale gestione dei quesiti da parte degli uffici competenti e la efficace chiusura del contatto con l'utente, ed eventualmente prevedere la disponibilita' di opportuni strumenti di e-mail management per agevolare e tracciare il processo.

Allegato n. 2
Organizzazione delle diverse fonti di rilevazione del gradimento degli utenti

Per quanto riguarda la modalita' diretta, la progettazione del questionario e delle altre forme di contatti va effettuata utilizzando adeguate metodologie che ne assicurino efficacia ed utilita'; inoltre e' importante rilevare non solo il gradimento espresso rispetto ai servizi disponibili, ma si deve rivolgere una particolare attenzione a quei servizi che costituiscono le principali aspettative future degli utenti. La conoscenza di servizi non ancora presenti, ma attesi, rappresenta un passo ulteriore di ausilio per la pianificazione di nuovi interventi. Le indicazioni vanno opportunamente confrontate con il potenziale bacino di utenza, con altri parametri inerenti i costi necessari per la loro realizzazione e con la loro concreta fattibilita'. Nella definizione dei rapporti «indiretti» occorre fare in modo che quanto proviene dagli utenti in termini di informazioni e indicazioni sia il piu' possibile strutturato, affinche' se ne possano trarre dei vantaggi in fase di analisi. Da qui l'importanza: a) che la strutturazione della interazione via e-mail sia orientata anche a rilevare la percezione dello scrivente; b) che l'operatore di contact center sia adeguatamente formato e sensibilizzato anche per far emergere criticita' ed aspettative, e che l'infrastruttura tecnologica consenta un'agevole e coerente tracciatura di tali informazioni; c) che le informazioni tratte dai due canali confluiscano in un database integrato. Nella misurazione delle caratteristiche tecniche di utilizzo dei servizi, si devono rilevare il numero di accessi necessari per individuare la transazione desiderata, il numero di pagine visitate per unita' di tempo, il numero di sessioni, la percentuale e la fase di «abbandono» lungo i percorsi di fruizione dei diversi

servizi (ad esempio, nel caso in cui si ricorra a componenti on-line solo per estrarre informazioni, realizzando l'interazione con modalita' tradizionali, e' ragionevole ipotizzare che l'esigenza esiste, ma la modalita' di erogazione della transazione e' inadeguata). Altra informazione interessante e' la distribuzione degli accessi nel tempo e, soprattutto, la percentuale degli accessi di nuovi utenti rispetto al totale, che costituisce un significativo indice di fidelizzazione e quindi di gradimento. La misurazione dell'utilizzo del servizio si puo' articolare in numero di accessi totali, in media giornaliera, in valore massimo e valore minimo degli stessi. Inoltre si puo' definire il numero degli accessi in prospettiva longitudinale (ad esempio numero riscontrato nell'ultimo mese, nei due mesi, sei mesi e dodici mesi precedenti). Questa ulteriore articolazione permettera' di rilevare l'andamento del servizio on-line ed eventuali aumenti o diminuzioni in rapporto a modifiche del servizio erogato on-line e, soprattutto, al livello di fruizione su altri canali. I dati rilevati devono essere organizzati in un'apposita base dati con profondita' storica, per analizzarne gli andamenti nel tempo e per operare confronti tra analoghe tipologie di servizi, comprensiva anche delle analisi effettuate sulle e-mail e sulle chiamate al contact center. Tale base informativa rappresenta uno strumento essenziale per la pianificazione strategica e tecnica dei nuovi interventi e quindi deve essere predisposta in maniera da consentire un accesso agevole, mirato e tempestivo alle informazioni per i diversi livelli operativi e decisionali dell'amministrazione.

Presentato a Roma il terzo rapporto sull'innovazione tecnologica nelle regioni e negli enti locali.

NUMERO SCHEDA: 6391

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: CNIPA

E' stato presentato nel corso della Conferenza dal titolo “L’innovazione tecnologica per il federalismo efficiente”, che si é tenuta il 30 giugno e il 1 luglio 2005 a Roma, il terzo “Rapporto sull’innovazione nelle regioni e negli enti locali” che segna il bilancio e i passi in avanti nell’attuazione dell’e-government in Italia.

Fotografa il coinvolgimento delle Regioni e degli Enti locali nei processi di innovazione, ad un anno dalla pubblicazione degli avvisi di cofinanziamento relativi alla II fase di e-government.

Il rapporto risulta così articolato:

- Introduzione.
- Parte I Quadro generale e lettura trasversale dei rapporti regionali.

1. L'innovazione nelle regioni: novità e sviluppi recenti.
2. Gli accordi di programma quadro per la società dell'informazione.
3. La revisione di medio periodo del qcs ob.1 e la società dell'informazione.
4. Avanzamento dei progetti 1° avviso.
5. L'avvio della fase 2 dell'e-government.
6. I progetti per cittadinanza elettronica.
7. Sviluppi del sistema pubblico di connevità e cooperazione.
8. La diffusione delle carte per l'accesso ai servizi.
9. I servizi on line per cittadini e imprese: un'analisi quantitativa sui comuni.

10. L'evoluzione della rete dei centri regionali di competenza per l'e-government e la società dell'informazione.
- Parte II Schede regionali di sintesi-
- Parte III. Indagine sulle policy di e-learning nelle regioni e province autonome.
- I risultati dell'indagine: l'e-learning nelle regioni.

Il rapporto, che è scaricabile al sito http://www.cnipa.gov.it, è in visione presso il settore Studi e documentazione legislativi.

Presentato il rapporto annuale del CNIPA sull'attività svolta e sullo stato di informatizzazione della P.A.

NUMERO SCHEDA: 6390

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

NATURA ATTO: RAPPORTO

A Roma, in data 5 luglio 2005, è stata presentata la Relazione annuale del Cnipa, edizione 2004, dal Presidente Livio Zoffoli presso il Complesso monumentale del Santo Spirito.
Il Rapporto illustra in modo dettagliato l'attività svolta dal Cnipa nell'anno precedente (Vol. I) e lo stato dell'informatizzazione nella Pubblica Amministrazione (Vol. II). Il rapporto è consultabile on line nella sezione dedicata alle Pubblicazioni del Cnipa.

Il rapporto, che è scaricabile al sito http://www.cnipa.gov.it, è in visione presso il settore Studi e documentazione legislativi.

In Gazzetta ufficiale il d.p.c.m. 31 maggio 2005 "Razionalizzazione in merito all'uso delle applicazioni informatiche e servizi ex articolo 1, commi 192, 193 e 194 della legge n. 311 del 2004 (Finanziaria 2005).

NUMERO SCHEDA: 6387

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: GAZZETTA UFFICIALE

NUMERO: 140

DATA: 18/06/2005

RIFERIMENTO NORMATIVO: art. 192 e art. 194 della legge n. 311 del 2005 (legge finanziaria 2005)

NATURA ATTO: DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

DATA ATTO: 31/05/2005

In attuazione dei commi 192 e 194 della legge n. 311 del 2004 (legge finanziaria 2005), è stato pubblicato il d.p.c.m. 31 maggio 2005 (G.U. del 18 giugno 2005, n. 140) predisposto dal Ministero per l'Innovazione Tecnologica con la collaborazione del CNIPA.
La Legge finanziaria 2005 ha previsto misure per migliorare l'efficienza operativa della PA e per il contenimento della spesa pubblica, rispettivamente ai commi 192 (razionalizzazioni ed eliminazioni di duplicazioni e sovrapposizioni di applicazioni e servizi informatici e riguardanti il funzionamento degli uffici) e 194 (interventi di razionalizzazione delle infrastrutture di calcolo, telematiche e di comunicazione delle amministrazioni).
La norma identifica da una parte le aree di intervento dei sistemi informativi del funzionamento: protocollo e gestione documentale; contabilità e controllo strategico; personale; uffici legislativi; formazione in modalità e-learning; servizi tecnici di natura strumentale. Dall'altra le categorie di interventi di razionalizzazione: CED principali di disaster recovery; infrastrutture, sistemi e servizi di comunicazione.

Si allega il testo.

Si segnala un interessante commento alla sentenza sulla rivista "Guida agli Enti Locali", n. 34 del 3 settembre 2005, pp. 48-49, in visione presso il settore Studi e documentazione legislativi.
Si tratta di un articolo, a cura di Paolo Subioli, intitolato "L'utilizzazione condivisa che porta i risparmi".

D.P.C.M. 31 maggio 2005 (1).

1. *Finalità.*
1. Il presente decreto individua le applicazioni informatiche ed i servizi per i quali si rendono necessarie razionalizzazioni ed eliminazioni di duplicazioni e sovrapposizioni, nonché gli interventi di razionalizzazione delle infrastrutture di calcolo, telematiche e di comunicazione delle amministrazioni di cui all'art. 1, del *decreto legislativo 12 febbraio 1993, n. 39*, al fine di migliorare l'efficienza operativa della pubblica amministrazione e per il contenimento della spesa pubblica.
2. Il presente decreto non si applica alle amministrazioni di cui all'art. 1 del *decreto legislativo 12 febbraio 1993, n. 39*, limitatamente all'esercizio delle sole funzioni di sicurezza e difesa nazionale, salva la facoltà delle amministrazioni interessate di richiederne l'applicazione.
2. *Individuazione di applicazioni informatiche e di servizi di competenza statale.*
1. Gli obiettivi di miglioramento dell'efficienza operativa della pubblica amministrazione e di contenimento della spesa pubblica da conseguire attraverso le razionalizzazioni e l'eliminazione di duplicazioni e sovrapposizioni, relativamente al funzionamento degli uffici, sono perseguiti mediante:
a) la realizzazione di nuove applicazioni informatiche idonee a soddisfare le esigenze di più amministrazioni;
b) il riuso, previo adattamento ed estensione alle esigenze di più amministrazioni, di applicazioni informatiche esistenti di proprietà di pubbliche amministrazioni;

c) l'utilizzo di servizi applicativi distribuiti in modalità ASP (Application Service Provider) da rendere disponibili a più amministrazioni; i servizi sono erogati anche attraverso l'impiego delle applicazioni informatiche di cui alle lettere *a*) e *b*).
2. Le applicazioni informatiche e i servizi applicativi da realizzare nelle modalità di cui al comma 1 sono le seguenti:
a) protocollo informatico e gestione documentale, inclusa la trasformazione della documentazione cartacea in digitale;
b) contabilità finanziaria per tutti i soggetti contabili in Italia (amministrazioni in regime ordinario, funzionari delegati e contabilità speciali), con l'adozione della firma digitale e la conseguente dematerializzazione di tutti i titoli di spesa;
c) contabilità economico-patrimoniale e controllo di gestione con sistemi omogenei di classificazione delle spese e dei costi;
d) controllo strategico e monitoraggio dell'attuazione del programma di Governo;
e) gestione giuridica e amministrativa del personale in servizio in Italia;
f) gestione delle competenze fisse e accessorie del personale, da integrarsi in un unico sistema retributivo e con la distribuzione in rete delle distinte delle competenze mensili del personale;
g) informatizzazione dell'attività degli uffici legislativi.
3. Ulteriore strumento di razionalizzazione e di contenimento della spesa è costituito dall'utilizzazione comune da parte delle amministrazioni dei seguenti servizi:
a) servizi di formazione del personale erogati con metodologie e tecnologie di *e-learning*, su una piattaforma tecnologica unitaria fruibile in ASP sulla quale progettare e sviluppare contenuti formativi di interesse specifico delle singole amministrazioni e di interesse comune a più amministrazioni, che le stesse utilizzano coerentemente con i piani di formazione di cui all'art. 7-*bis* del *decreto legislativo 30 marzo 2001, n. 165*;
b) servizi di gestione e conduzione tecnica e operativa dei sistemi informatici e delle reti, servizi di help desk, servizi di messaggistica, servizi di hosting e servizi redazionali dei siti web;
c) servizi di supporto ai «Call center» che rendano disponibili in ASP piattaforme unitarie per la gestione dei contenuti e dei contatti con gli utenti.
4. Per le applicazioni informatiche e per i servizi di cui al presente articolo il Centro nazionale per l'informatica nella pubblica amministrazione (di seguito: CNIPA) stipula i contratti quadro di cui all'art. 1, comma 192, della *legge n. 311 del 2004*.
3. *Individuazione di infrastrutture di competenza statale.*
1. Gli obiettivi di miglioramento dell'efficienza operativa della pubblica amministrazione e di contenimento della spesa pubblica sono conseguiti mediante interventi di razionalizzazione di infrastrutture di calcolo, telematiche e di comunicazioni delle amministrazioni di cui all'art. 1 del *decreto legislativo 12 febbraio 1993, n. 39*, anche con l'introduzione di nuove tecnologie e servizi. Gli interventi riguardano:
a) centri elaborazione dati (CED) di cui razionalizzare, ottimizzare e riallocare sul territorio le strutture esistenti, eliminando duplicazioni derivanti anche da intervenuti accorpamenti di Ministeri;
b) infrastrutture, sistemi e servizi di comunicazione, da migliorare e razionalizzare mediante interventi che favoriscano l'utilizzo delle nuove tecnologie fra cui la telefonia VoIP (Voice over Internet Protocol), le tecnologie senza fili «wireless» e i servizi pubblici su reti mobili;
c) centri per garantire la salvaguardia dei dati e delle applicazioni informatiche e la continuità operativa dei servizi informatici e telematici, anche in caso di disastri e di situazioni di emergenza, attraverso la definizione di infrastrutture, sistemi e servizi comuni a più amministrazioni, anche utilizzando CED già esistenti.
2. Il CNIPA, ai fini di cui al comma 1, svolge funzioni di impulso e coordinamento, anche attraverso l'indizione di conferenze di servizi.
4. *Attuazione e monitoraggio.*
1. Il CNIPA, per il perseguimento degli obiettivi di cui all'art. 1, tenendo presenti anche le proposte delle amministrazioni formulate ai fini della predisposizione del piano triennale di cui all'art. 9 del *decreto legislativo 12 febbraio 1993, n. 39*, e sentita la Ragioneria generale dello Stato, entro il 30 giugno di ciascun anno propone al Presidente del Consiglio dei Ministri o al Ministro delegato per l'innovazione e le tecnologie un programma di interventi.
2. Il programma di cui al comma 1, dopo l'approvazione da parte del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, è inviato alle amministrazioni di cui all'art. 1 del

decreto legislativo 12 febbraio 1993, n. 39, ed è recepito nelle direttive annuali per l'azione amministrativa di cui all'art. 14 del *decreto legislativo 30 marzo 2001, n. 165*.
3. Il CNIPA assiste le amministrazioni nella realizzazione degli stessi, monitorandone, in collaborazione con le amministrazioni interessate, l'attuazione ed i risultati; sui medesimi risultati riferisce al Presidente del Consiglio dei Ministri o al Ministro per l'innovazione e le tecnologie con rapporti periodici e con una relazione annuale da predisporsi entro il 31 gennaio dell'anno successivo.
4. Entro il 31 gennaio di ciascun anno il CNIPA invia, per il tramite della Presidenza del Consiglio dei Ministri, al Ministro dell'economia e delle finanze un rapporto sui risparmi di spesa ottenuti nell'anno precedente e sui risparmi previsti nell'anno in corso.
5. Le pubbliche amministrazioni interessate adottano i provvedimenti necessari per dare attuazione al presente decreto.
Il presente decreto è trasmesso ai competenti organi di controllo e pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

In Consiglio regionale del Piemonte avviata la discussione di due progetti di legge in materia di ricerca e innovazione.

NUMERO SCHEDA: 6338

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

NATURA ATTO: PROGETTO DI LEGGE

DATA ATTO: 2004

NUM. ATTO: 648/2004 e 664/2004

Presso il Consiglio regionale del Piemonte sono state presentate due proposte di legge in materia di ricerca ed innovazione tecnologica.
Si tratta della pdl n. 648/2004 (Sistema ricerca, innovazione e sviluppo del Piemonte e reti di conoscenza) e del ddl n. 664/2004 (Sistema regionale della ricerca).
I due progetti sono stati analizzati dalle competenti commissioni in un testo unificato.

Si riporta il testo.

Proposta di legge regionale n. 648 presentata il 08 luglio 2004
Sistema ricerca, innovazione e sviluppo del Piemonte e reti della conoscenza.

Titolo I.
FINALITÀ E SISTEMA REGIONALE RICERCA INNOVAZIONE E SVILUPPO

Art. 1
(Finalità e Sistema regionale ricerca innovazione e sviluppo)

1.La Regione Piemonte, nel rispetto dei principi di libertà della scienza e dell'autonomia delle Istituzioni dell'alta cultura e dell'università di cui all' articolo 33 della Costituzione e in armonia con gli indirizzi della

programmazione nazionale ed europea tesi a realizzare lo ¿Spazio Europeo della ricerca e dell'innovazione¿, promuove e coordina azioni per lo sviluppo della ricerca, l'innovazione e il trasferimento tecnologico al sistema produttivo nell'esercizio della propria potestà legislativa in materia prevista dall' articolo 117, comma terzo della Costituzione e delle funzioni conferite dall' articolo 19 del decreto legislativo 31 marzo 1998, n. 112.
2.La presente legge è finalizzata allo sviluppo complessivo del sistema regionale della ricerca e dell'innovazione, di seguito definito ¿sistema regionale ricerca innovazione e sviluppo¿, alla costruzione della dimensione regionale della ricerca, al potenziamento delle reti della conoscenza e delle reti dell'innovazione ed alla valorizzazione del ciclo ricerca-formazione-innovazione-sviluppo, ai fini del più generale sviluppo della società regionale e dell'economia della conoscenza.
3.Gli interventi nei settori di competenza regionale per i quali si applica specifica normativa regionale sono raccordati a quelli previsti dalla presente legge per realizzare in modo coerente ed integrato le finalità di sviluppo del sistema ricerca e innovazione nella dimensione regionale.

Art. 2
(Modello cooperativo. Soggetti del sistema regionale ricerca innovazione e sviluppo. Azioni e Metodologia)

1.Per il raggiungimento delle finalità di cui all'articolo 1, la Regione Piemonte, nell'ambito delle proprie competenze e nel rispetto dell'autonomia dei soggetti con proprie competenze in materia di ricerca e innovazione e di quelli operanti in tale campo, svolge la propria azione di promozione e coordinamento attraverso un modello di cooperazione istituzionale ai vari livelli e dimensioni e di interazione tra i soggetti pubblici e privati e le rispettive risorse istituzionali, economiche, culturali, sociali, finanziarie e strumentali disponibili e necessarie allo sviluppo del sistema regionale ricerca e innovazione.
2.I soggetti che concorrono in modo organico allo sviluppo della dimensione regionale della ricerca e che partecipano in una logica di sistema alla realizzazione delle finalità di cui all'articolo 1 e al consolidamento del sistema regionale ricerca innovazione e sviluppo sono, in generale: le istituzioni e autonomie locali e territoriali, le istituzioni universitarie, gli enti e centri di ricerca pubblici e privati, i parchi scientifici e tecnologici e i distretti tecnologici territoriali, imprese, consorzi e società consortili miste tra impresa, istituzioni universitarie e della ricerca, associazioni economiche, produttive e di categoria, fondazioni ex bancarie e sistema creditizio, enti strumentali della Regione, sistema sanitario e sistema culturale e sociale.
3.Le finalità di cui all'articolo 1 si realizzano attraverso azioni principali incentrate sulla connessione tra ricerca, formazione, innovazione, impresa e modello di sviluppo, volte in particolare a:
a)sostenere l'alta formazione nei confronti dei giovani per attrarre e motivare un numero crescente di giovani verso le attività di ricerca e innovazione e ad alto contenuto di conoscenza;
b)realizzare infrastrutture immateriali intese come reti di formazione del sapere che costituiscano elementi di organizzazione e di supporto alle attività;
c)realizzare nei diversi ambiti territoriali le attività innovative attraverso la messa in contatto dei soggetti coinvolti per i propri ambiti di competenza e di autonomia nello sviluppo del sistema regionale e nella realizzazione degli interventi;
d)creare attraverso la ricerca nuove opportunità in settori ritenuti strategici ma da potenziare in Piemonte, come leva fondamentale per aprire nuove aree attrattive per soggetti piemontesi e soprattutto a livello di Comunità Europea.
4.Al fine di operare in una logica di sistema, la Regione Piemonte, in particolare, valorizza:
a)i risultati degli interventi nei diversi settori di competenza regionale e di quelli conseguiti dagli enti strumentali della Regione;
b)l'apporto di iniziative e di soggetti sostenuti da fondi privati, tra cui le Fondazioni ex bancarie e il sistema creditizio, affinché la propria autonomia progettuale sia valorizzata e orientata verso il sistema ricerca e innovazione;
c)l'apporto di idee e sapere interdisciplinare delle istituzioni universitarie e dei centri di ricerca.
5.La metodologia individuata per operare secondo tale logica di sistema si basa su due elementi tra loro collegati:
a)aggregazione fra i soggetti fondamentali del sistema su cui si costruisce l'interdisciplinarietà degli interventi e il concorso di una pluralità di soggetti:

1)l'utente e/o il committente della attività innovativa;
2)l'impresa o il soggetto economico che intende introdurre all'interno della propria attività l'innovazione;
3)il centro di ricerca portatore di contenuti di innovazione e ricerca;
4)i soggetti impegnati nel processo di accrescimento della conoscenza che costituiscono il veicolo del trasferimento di tecnologie;
b)integrazione delle risorse pubbliche e private (o matching funds) individuate per l'attivazione dell'intervento e su cui si costruisce l'interazione fra i soggetti coinvolti, anche al fine di realizzare interventi di scala adeguata e di favorire la partecipazione a bandi europei.

Art. 3 (Il mondo della ricerca)

1.La Regione Piemonte riconosce il mondo della ricerca quale soggetto fondamentale e centrale ai fini della crescita del sistema regionale ricerca innovazione e sviluppo.
2.Per il potenziamento del mondo della ricerca la Regione Piemonte promuove, nell'ambito delle azioni di cui all'articolo 2, interventi e iniziative specifiche per:
a)favorire la condivisione di risorse sia intellettuali, sia finanziarie, sia operative e la convergenza tra ambiti disciplinari e di ricerca;
b)favorire la comunicazione fra diverse aree di ricerca, creare un linguaggio e infrastrutture in comune e costruire una rete di collegamento tra l'alta formazione, i centri di ricerca e di eccellenza e le agenzie e tra i soggetti fondamentali della ricerca per la collaborazione attiva e per lo scambio di conoscenze.
3.La metodologia individuata per operare in un'ottica di sistema è tesa ad assicurare, dal lato delle risorse del mondo della ricerca, la convergenza delle diverse risorse culturali già presenti e per lo più organizzate in termini disciplinari e, dal lato delle risorse dei diversi ambiti funzionali e di competenza, il coordinamento delle risorse economiche attualmente impiegate a cui ricondurre anche quelle sottoposte a vincoli di destinazione attraverso le iniziative e le procedure necessarie.

Titolo II.STRUMENTI DI PROGRAMMAZIONE E DI INTERVENTO

Art. 4
(Indirizzi di programmazione e intervento)

1.La Regione Piemonte attraverso strumenti di programmazione e di intervento promuove e coordina la crescita del sistema ricerca innovazione e sviluppo di cui all'articolo 1, secondo gli indirizzi di seguito delineati:
a)convergenza delle politiche di ricerca e innovazione con quelle a livello nazionale e comunitario ai fini di una armonizzazione con gli indirizzi e gli strumenti di programmazione e di intervento e di un coordinamento delle attività e dei mezzi disponibili e del più ampio concorso al conseguimento delle misure e dei risultati anche attraverso iniziative e accordi a carattere interregionale;
b)cooperazione dei soggetti istituzionali, delle autonomie locali e territoriali nel territorio della Regione e ai livelli nazionale ed europeo;
c)cooperazione/interazione fra i soggetti istituzionali, economici, sociali, culturali e della ricerca e alta formazione per implementare il sistema anche ai fini della definizione di un modello condiviso e largamente applicato e di una sistematica valutazione dei risultati;
d)trasversalità e interdisciplinarietà della ricerca e interazione/integrazione fra ricerca di base e applicata, quale leva per la crescita della società e dell'economia della conoscenza;
e) valorizzazione della tecnostruttura pubblica (università e centri di ricerca) e del sistema finanziario e interazione/integrazione fra tecnostruttura e sistema delle imprese per valorizzare e fluidificare il ciclo ricerca-formazione-innovazione-sviluppo;
f)organicità e sistematicità degli interventi di investimento in capitale umano e qualità della formazione (standard e didattica) e in infrastrutture immateriali come reti di formazione del sapere e non solo tecnologiche per potenziare il sistema e la dimensione regionale della ricerca;
g)integrazione fra politiche di intervento settoriale, misure e strumenti per lo sviluppo della ricerca e dell'innovazione e integrazione delle risorse e dei mezzi disponibili ai fini di conseguire risultati di sistema

attraverso il coordinamento delle attività, l'interdisciplinarietà della ricerca e l'interazione/cooperazione fra istituzioni, università e centri di ricerca, imprese, agenzie culturali e sociali ed enti strumentali;
h)potenziamento della rete regionale della ricerca e suo inserimento nelle reti globali della produzione del sapere per potenziare le conoscenze e le risorse e sviluppo delle reti della conoscenza e delle reti dell'innovazione;
i)comunicazione e diffusione della cultura della ricerca nel contesto della società e dell'economia della conoscenza e promozione di servizi di informazione e di azioni per favorire la diffusione dei programmi di intervento, lo scambio di conoscenze fra il mondo accademico e non e le interazioni fra il mondo della ricerca e quello dell'industria e dei servizi, in particolare, quelli ad alta intensità di conoscenza generale e tecnologica;
j)divulgazione scientifica per favorire l'aggiornamento continuo dei soggetti e la crescita delle capacità di acquisire competenze e metodologie per tutto l'arco della vita.

Art. 5
(Programmi triennale ed annuale per lo sviluppo del sistema regionale ricerca innovazione e sviluppo. Procedure di approvazione e valutazione)

1.Il Consiglio regionale, su proposta della Giunta regionale, per le finalità di cui all'articolo 1, approva il programma triennale per la crescita del sistema regionale ricerca e innovazione e sviluppo.
2.Il programma triennale, in coerenza con gli indirizzi di cui all'articolo 4, in particolare:
a)specifica le azioni principali di cui all'articolo 2 e i relativi strumenti e individua gli interventi e le relative aree e tipologie e i settori strategici, anche quelli da strutturare, in modo coerente ed integrato con gli interventi previsti da specifica normativa regionale, per l'innovazione d'impresa o di prodotto e servizio, per i nuovi settori o per le nuove imprese innovative avviate anche con il supporto dell'università, dei centri di ricerca e dei centri di innovazione e trasferimento tecnologico o per le iniziative ad alto valore conoscitivo;
b)esplicita l'aggregazione fra i soggetti fondamentali del sistema e l'integrazione delle risorse pubbliche e private su cui si attivano gli interventi per lo sviluppo del sistema e l'interazione fra i soggetti coinvolti;
c)individua le risorse integrative e quantifica le risorse finanziarie complessive, pubbliche e private esplicitamente rivolte ad attività di ricerca e di innovazione e ad alto contenuto di conoscenza, anche in armonia con gli indirizzi contenuti nel Documento di programmazione economico-finanziaria;
d)aggiorna gli indirizzi di programmazione di cui all'articolo 4 in relazione alle mutate esigenze del contesto di riferimento ed agli indirizzi di programmazione e direttive nazionali ed europei.
3.La proposta di programma triennale è presentata e approvata contestualmente alla presentazione del Documento di programmazione economico-finanziaria, nel primo anno di ciascun triennio di riferimento.
4.La Giunta regionale, sulla base del programma regionale triennale approvato dal Consiglio regionale, approva un programma operativo annuale quale articolazione del piano triennale. Il programma operativo specifica, in riferimento a ciascuna azione, l'attribuzione degli stanziamenti per i diversi interventi, le tipologie di finanziamento e le relative modalità di assegnazione ed erogazione, i requisiti di ammissibilità e i soggetti destinatari degli interventi e ogni altra clausola necessaria per l'operatività del programma stesso.
5.La Giunta regionale annualmente invia al Consiglio regionale una relazione sullo stato di attuazione del programma annuale e al termine del triennio di riferimento un rapporto sull'attuazione del programma triennale e sugli indicatori di risultato relativi a ciascuna azione di cui all'articolo 2. Detti documenti sono comunicati anche alla Conferenza permanente Regione Autonomie locali.

Art. 6
(Fondo Unico Regionale per lo sviluppo del sistema ricerca e innovazione)

1.È istituito il Fondo Unico Regionale per lo sviluppo del sistema ricerca e innovazione, strutturato in due Fondi per la spesa di parte corrente e per la spesa di parte d'investimento.
2.Detto Fondo contiene le risorse regionali disponibili costituite da:
a)risorse specifiche;

b)risorse impiegate nei settori di competenza regionale da riorientare verso interventi di ricerca e a maggiore valore conoscitivo, ferme restando quelle già esplicitamente rivolte alla ricerca;
c)donazioni liberali alla ricerca;
d)risorse di fonte statale e di fonte comunitaria;
e)risorse provenienti da ritorni economici di cui al comma 3 dell'articolo 7.
3.Il Fondo unico è ripartito in relazione agli strumenti e alle tipologie di intervento indicati nel programma di cui all'articolo 5.
4.All'assetto complessivo del Fondo, in forma descrittiva, concorrono le risorse regionali di cui al comma 2 e le risorse di fonte privata esplicitamente riferite ad attività di ricerca e di innovazione, tra cui quelle del settore creditizio e delle fondazioni ex bancarie e le risorse proprie degli enti strumentali della Regione, che in modo integrato con le risorse regionali, costituiscono l'ammontare complessivo del Fondo da destinare al finanziamento degli interventi programmati.

Art. 7
(Flusso gestionale del Fondo)

1.La Regione Piemonte, con riferimento al programma e alla dotazione complessiva del Fondo, assegna le risorse finanziarie sulla base di un bando aperto al quale concorrono i soggetti che propongono iniziative progettuali rispondenti agli interventi programmati e ai settori strategici individuati nel programma di cui all'articolo 5 e che documentino i seguenti requisiti principali per la selezione, specificati con dettaglio nel bando:
a)la dimensione del cofinanziamento, anche ripartito tra soggetti diversi;
b)il ritorno atteso della attività proposta;
c)le metriche di valutazione e di misura dei risultati.
2.I finanziamenti sono divisi in quote. L' erogazione delle quote successive alla prima è condizionata alla presentazione di una relazione che dimostri lo stato d'avanzamento della ricerca, da rendere pubblica in ogni fase realizzativa per assicurarne il controllo.
3.
Possono, previ accordi di negoziazione tra la Regione Piemonte e le parti interessate in sede di finanziamento di specifici progetti di ricerca, essere definiti eventuali ritorni economici (ad esempio royalties o sfruttamento di brevetti) da destinare ad impinguare il Fondo di cui all'articolo 6.

Art. 8
(Interventi per lo sviluppo del sistema ricerca e innovazione)

1.Gli interventi per lo sviluppo del sistema ricerca e innovazione sono individuati in coerenza con le azioni di cui all'articolo 2, al fine di realizzare investimenti sulle risorse umane, sulle infrastrutture immateriali, sull'innovazione nel territorio e su settori strategici.
2.Gli interventi finalizzati allo sviluppo del sistema riguardano in particolare:
a)l'istituzione di borse per giovani, di cui all'articolo 9;
b)l'implementazione di infrastrutture immateriali, di cui all'articolo 10;
c)l'attivazione di accordi territoriali, al fine di valorizzare luoghi, ambiti territoriali, unità immobiliari sotto utilizzate e l'innovazione produttiva anche nel contesto dei piani di sviluppo locali;
d)la promozione di attività culturali e di scambio di conoscenze fra il mondo accademico, della ricerca e dell'impresa, quali seminari, workshop, conferenza annuale su ricerca, formazione, innovazione e sviluppo.

Art. 9
(Borse per giovani ricercatori e altri interventi)

1.Le borse sono rivolte ai giovani ricercatori dell'Unione Europea, fino a ventinove anni, che operino in una realtà di ricerca sul territorio piemontese per elevare il dimensionamento e la qualità della ricerca in Piemonte.

2.La Regione cofinanzia le borse fino ad un massimo del 50 per cento e, in tal caso, le borse sono definite Borse Regione Piemonte¿. In caso di finanziamento regionale inferiore è previsto un marchio Regione Piemonte¿ da aggiungere al brand del soggetto finanziatore principale.
3.La Regione favorisce l'attuazione di interventi complementari e integrativi individuati nell'ambito del programma triennale, con riferimento all'assetto integrato del Fondo. Tali interventi possono essere finalizzati all'estensione dell'entità di borse di dottorato, all'allargamento degli interventi per il diritto allo studio a favore dei dottorandi, al finanziamento di specifici progetti per giovani ricercatori, di stage o scambi o di corsi congiunti tra ricerca e impresa, all'integrazione negli indirizzi programmatici della formazione professionale di misure rivolte al potenziamento della ricerca e al raccordo con le imprese, ed alla promozione di ogni altro intervento per accrescere l'investimento in capitale umano.

Art. 10
(Infrastrutture immateriali e reti della conoscenza e dell'innovazione)

1.La Regione Piemonte, per potenziare le reti della conoscenza e rafforzare i nodi della rete dell'innovazione e lo sviluppo del territorio e di nuovi prodotti e servizi, promuove l'implementazione di infrastrutture immateriali attraverso i seguenti interventi:
a)creazione di laboratori dell'innovazione o potenziamento di laboratori esistenti, come attività immateriale che integra ricerca, impresa e territorio secondo gli interventi specificati nel programma di cui all'articolo 4, da rendere disponibili all'intero sistema attraverso varie forme di utilizzo in condivisione;
b)strutture finanziarie e di consulenza finalizzate al supporto alla ricerca;
c)evoluzione della Rete Unitaria della Pubblica Amministrazione Regionale (RUPAR) verso una rete capace di sostenere la ricerca e l'interazione fra il mondo della ricerca e quello delle imprese, anche in cooperazione con la rete GARR;
d)definizione di strumenti software applicativi sulla RUPAR specializzati per funzioni di particolare rilievo, quali un sistema di teledidattica, un sistema di archiviazione e produzione di informazioni multimediali, l'accesso a basi di dati speciali, sistemi cooperativi, strutture di calcolo distribuite ed altri interventi affini.

Art. 11
(Organismi e strumenti di coordinamento e di governo del sistema)

1.Ai fini dello sviluppo e del governo del sistema la Regione Piemonte si avvale di organismi di coordinamento e di consulenza, di cui ai commi 2 e 5.
2.È istituito il Coordinamento ricerca innovazione e sviluppo per la ricerca e l'innovazione, i cui componenti sono designati da: Regione Piemonte, Atenei Piemontesi, Enti Locali, Enti strumentali regionali, Enti e centri di ricerca pubblici e privati rappresentativi a livello nazionale, localizzati sul territorio piemontese, Fondazioni ex bancarie, Associazioni maggiormente rappresentative delle attività economiche, produttive e di categoria, Unione Europea e Ministero competente.
3.La Giunta regionale con proprio atto deliberativo definisce i criteri e le modalità per la designazione e la nomina dei componenti il Coordinamento e individua ulteriori componenti tra i soggetti di cui all'articolo 2, comma 2.
4.Il Coordinamento opera in raccordo con il Comitato Scientifico di cui al comma 7, e ha funzioni di:
a)supporto al governo del sistema e alla attività di programmazione per individuare gli interventi, le relative aree e tipologie e i settori strategici ai fini della predisposizione del programma di cui all'articolo 4;
b)consulenza e proposta alla Giunta regionale per favorire la cooperazione tra i soggetti del sistema e per coordinare e promuovere la ricerca l'innovazione e lo sviluppo in un'ottica di sistema, anche attraverso strumenti di consultazione e di indagine sul territorio e nella comunità regionale;
c)monitoraggio degli esiti degli interventi di cui al programma operativo annuale da fornire al Comitato Scientifico e alla Giunta regionale;
d)comitato guida per i canali di comunicazione e divulgazione, quale momento di promozione e documentazione dell'attività.
5.Presiede il Coordinamento il Presidente della Giunta regionale o l'Assessore delegato competente.
6.La struttura regionale competente svolge le funzioni di Segreteria e di supporto all'attività del Coordinamento e cura le attività relative al flusso gestionale del Fondo di cui all'articolo 7, in funzione del

governo del sistema e della predisposizione della documentazione necessaria per l'attività del Consiglio e della Giunta regionale.
7.È istituito il Comitato scientifico per la ricerca innovazione e sviluppo (di seguito denominato Comitato scientifico) composto da cinque componenti di alto profilo scientifico e culturale, operanti nel territorio piemontese e nominati per il triennio di riferimento dal Consiglio regionale. I suoi componenti sono rieleggibili per non più di due volte consecutive; il Comitato scientifico elegge al proprio interno il Presidente, il quale convoca il Comitato almeno una volta all'anno o quando sia richiesto dal Presidente della Giunta regionale. Il Comitato scientifico decade, comunque, al termine della legislatura.
8.Il Comitato scientifico ha funzioni di proposta e consulenza generale e di analisi di scenario e di valutazione ex ante delle linee di intervento ed ex post dell'impatto degli interventi e dei risultati del programma triennale e del programma operativo annuale. Inoltre attiva rapporti e collegamenti con soggetti di alta competenza scientifica e culturale, operanti a livello nazionale, europeo e internazionale, ai fini delle funzioni di analisi e valutazione ex ante ed ex post.
9.La struttura regionale competente di cui al comma 6 svolge le funzioni di Segreteria .
10.I compensi a favore dei componenti il Comitato scientifico sono definiti con atto deliberativo della Giunta regionale.

Titolo III.NORME D'ATTUAZIONE

Art. 12
(Istituzione di una nuova struttura regionale)

1.Per il finanziamento delle iniziative previste dalla presente legge si provvede mediante l'istituzione di una nuova unità previsionale di base, collocata all'interno della direzione programmazione economica, a tale unità previsionale di base corrisponde un nuovo settore da istituirsi secondo le modalità previste dalla legge regionale 8 agosto 1997, n. 51 (Norme sull'organizzazione degli uffici e sull' ordinamento del personale regionale) tale settore assume le funzioni di coordinamento di tutte le iniziative predisposte dalla Giunta regionale in materia di ricerca scientifica.

Art. 13
(Norma finanziaria)

1.Gli stanziamenti necessari per l'unità previsionale di base istituita ai sensi del precedente articolo sono iscritti nel bilancio della Regione con legge finanziaria regionale ai sensi di quanto previsto dall' articolo 8 della legge 7/2001e successive modificazioni.
2.La copertura finanziaria delle risorse da iscrivere nel bilancio della regione è assicurata, per gli anni 2005, 2006 e 2007 con utilizzo pari ad una percentuale del 5 per cento delle risorse introitate dalla regione quale compartecipazione regionale all'imposta sul valore aggiunto.
3.Per gli anni successivi si provvede ai sensi del secondo comma del presente articolo senza ulteriore vincolo.
4.Tali risorse sono integrate con quelle iscritte nel bilancio annuale della Regione per l'anno 2004 e nel bilancio pluriennale della Regione per gli anni 2005 e 2006 che finanziano le risorse trasferite o delegate dallo Stato, dall'Unione europea e dal sistema delle autonomie locali del Piemonte per il sostegno a specifici progetti di ricerca e con gli atri soggetti previsti dall'articolo 6.

Art. 14
(Disposizioni transitorie e finali)

1.Nel primo anno di attuazione della presente legge, qualora il Documento di programmazione economico-finanziaria sia già stato approvato, la Giunta regionale, entro il 31 ottobre 2004, approva e presenta al Consiglio regionale la proposta di deliberazione del programma triennale di cui all'articolo 5 per l'approvazione.

2.Fino alla istituzione della struttura regionale competente in materia di ricerca le funzioni di cui all'articolo 11, comma 6 sono attribuite alla struttura regionale competente in materia di programmazione e statistica.

Disegno di legge regionale n. 664 presentato il 29 Settembre 2004
Sistema regionale della ricerca.

Art. 1
(Finalità)

1.La Regione Piemonte, nell'esercizio della propria potestà legislativa in materia di ricerca scientifica e tecnologica a sostegno dell'innovazione per i sistemi produttivi, prevista dall' articolo 117 della Costituzione, ed al fine di esercitare le funzioni ad essa conferite, inerenti la realizzazione di programmi per la ricerca, l'innovazione ed il trasferimento tecnologico al sistema produttivo, secondo i principi dell' articolo 19 del decreto legislativo 31 marzo 1998 n. 112, promuove la creazione del "Sistema Regionale della Ricerca" all'interno dello "spazio europeo della ricerca", che assegna alle Regioni un ruolo di promozione e coordinamento delle conseguenti attività in ambito locale. In tale ambito la Regione riconosce il ruolo costituzionale attribuito alle Università dall' articolo 33 della Costituzione per la realizzazione delle finalità istituzionali pubbliche nel campo della didattica e della ricerca.
2.Ai fini della creazione del "Sistema Regionale della Ricerca" la Regione si propone di:
a)contribuire al progresso ed alla diffusione della ricerca nel campo scientifico, tecnologico, umanistico, economico e giuridico;
b)favorire lo sviluppo della competitività del sistema produttivo piemontese basato sulla conoscenza e sull'innovazione;
c)valorizzare e sostenere l'attività di ricerca svolta all'interno delle Università, del Politecnico, dei Centri di ricerca pubblici e privati, dei Parchi scientifici e tecnologici e delle imprese, favorendo le eccellenze, l'interdisciplinarietà e l'internazionalizzazione, in conformità con gli indirizzi emergenti a livello nazionale ed europeo;
d)favorire la messa in rete dei soggetti di cui alla lettera c), promuovendo forme di collaborazione fra pubblico e privato, anche ai fini del trasferimento di conoscenze, competenze e nuove tecnologie;
e)potenziare le strutture e gli strumenti della ricerca anche attraverso lo sviluppo di laboratori misti pubblico-privati e dei Centri d'innovazione nonché attraverso il potenziamento del patrimonio librario regionale;
f)promuovere l'utilizzo delle risorse umane, favorendo la mobilità dei ricercatori e l'impiego dei giovani nelle attività di ricerca;
g)valorizzare i risultati della ricerca anche ai fini della creazione di nuove imprese;
h)svolgere una costante azione di monitoraggio e di valutazione dei risultati sulla ricerca;
i)promuovere efficaci azioni di valutazione coerenti con i meccanismi di peer-review internazionalmente accettati;
l)sostenere la formazione di nuovi ricercatori e l'attrazione di talenti per la ricerca da altre regioni e nazioni.
Art. 2
(Sistema Regionale della Ricerca)

1.La Regione Piemonte, nell'ambito delle proprie competenze e nel rispetto dell'autonomia dei soggetti che operano nel campo della ricerca e dell'innovazione, promuove la creazione di un quadro di cooperazione finalizzato alla realizzazione del "Sistema Regionale della Ricerca", in aperta e costante interazione con il livello nazionale ed internazionale, nonché con tutti i soggetti rilevanti ai fini dello sviluppo regionale.
2.La Regione Piemonte promuove altresì la creazione del contesto più favorevole allo sviluppo del sistema produttivo locale, ponendolo nelle condizioni di trarre vantaggio dai cambiamenti indotti dalla tecnologia e dal progresso della conoscenza.
3.Concorrono volontariamente alla realizzazione del "Sistema Regionale della Ricerca" i soggetti che abbiano una stabile organizzazione nel territorio regionale e risultino compresi tra:

a)Università, Politecnico, Consiglio Nazionale delle Ricerche (CNR), enti di ricerca pubblici e privati, organismi pubblici e privati che abbiano come fine lo sviluppo di programmi per la ricerca, l'innovazione e il trasferimento tecnologico al sistema produttivo;
b)Parchi scientifici e tecnologici, distretti industriali;
c)Aziende sanitarie ospedaliere (ASO), Aziende sanitarie locali (ASL), società a prevalente partecipazione regionale ed enti strumentali della Regione che operino nel campo della ricerca;
d)imprese che esercitano l'attività di cui all'articolo 2195 del codice civile;
e)consorzi e società consortili costituiti da Regione, Università, Politecnico ed enti di ricerca con imprese, loro associazioni, organismi di ricerca.
4.Possono, altresì, contribuire alla promozione e al sostegno del "Sistema Regionale della Ricerca" le fondazioni di origine bancaria, gli enti locali, le camere di commercio, le associazioni di categoria ed i diversi soggetti che intendano contribuire allo sviluppo e alla diffusione della cultura e della conoscenza.

Art. 3
(Linee generali di intervento. Piano pluriennale della ricerca)

1.Il Consiglio regionale, coerentemente con gli indirizzi del Piano Nazionale della Ricerca e delle direttive europee in materia di ricerca, adotta, su proposta della Giunta, le linee generali d'intervento per il raggiungimento degli obiettivi di cui alla presente legge e fissa l'insieme delle risorse finanziarie occorrenti per l'attuazione delle medesime.
2.Sulla base delle linee fissate dal Consiglio regionale la Giunta adotta un piano pluriennale per la creazione e lo sviluppo del Sistema Regionale della Ricerca contenente: le aree d'intervento, l'indicazione delle azioni ritenute prioritarie, le categorie di soggetti beneficiari, le modalità di attuazione, gli strumenti e le tipologie d'intervento, i criteri di valutazione e l'allocazione, tenendo conto degli interventi in materia di ricerca finanziati in base a normative di settore, delle risorse disponibili sul fondo previsto dall'articolo 7 per singole aree di intervento. Il piano è suscettibile di revisione ed aggiornamento annuale da parte della Giunta.
3.La Giunta regionale con proprio provvedimento, in conformità alla normativa comunitaria e nel rispetto dei principi fondamentali desumibili dalla legislazione statale, anche al fine di garantire la trasparenza e la semplificazione delle procedure nonché la corrispondenza degli interventi alle esigenze del sistema nazionale della ricerca , disciplina i controlli, le revoche ed il monitoraggio dei finanziamenti concessi in applicazione della presente legge e, laddove non sia diversamente disciplinato, degli interventi attivati, in materia di ricerca, in base a normative di settore.
4.Gli interventi attuativi delle leggi settoriali in materia di ricerca devono risultare coerenti con i contenuti del piano pluriennale per la creazione e lo sviluppo del Sistema Regionale della Ricerca.
5.La Giunta invia annualmente al Consiglio regionale una relazione sullo stato di attuazione del piano pluriennale e, all'esito del periodo di vigenza, presenta la relazione sullo stato della ricerca in Piemonte in cui sono, tra l'altro, indicati gli obiettivi conseguiti in attuazione del piano.

Art. 4
(Comitato per la ricerca e l'innovazione)

1.È istituito il Comitato per la ricerca e l'innovazione.
2.Il Comitato è strumento di raccordo, consultazione e partecipazione della comunità regionale per l'elaborazione e l'attuazione delle politiche finalizzate alla creazione del sistema regionale della ricerca. Il Comitato, in particolare, contribuisce alla definizione delle linee del piano pluriennale e di iniziative di collaborazione dirette a favorire l'integrazione fra i soggetti che operano nell'ambito del "Sistema Regionale della Ricerca".
3.Il Comitato è composto da:
a)un rappresentante della Regione;
b)un rappresentante della Università degli Studi di Torino;
c)un rappresentante del Politecnico di Torino;
d)un rappresentante dell'Università degli Studi del Piemonte Orientale "Amedeo Avogadro";
e)un rappresentante del Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR);

f)un rappresentante della Fondazione Torino Wireless;
g)un rappresentante della Unioncamere Piemonte;
h)un rappresentante della Tecnorete Piemonte S.c.a.r.l;
i)un rappresentante della Compagnia di San Paolo;
l)un rappresentante della Fondazione Cassa di Risparmio di Torino;
m)un rappresentante della Associazione delle Fondazioni delle Casse di risparmio piemontesi;
n)un rappresentante di Confindustria Piemonte;
o)un rappresentante della Federapi;
p)un rappresentante del CNR;
q)un rappresentante del Centro Ricerche FIAT (CRF);
r)un rappresentante della Telecom Italia Lab;
s)un rappresentante dell'Istituto "Guido Donegani" di Novara.
4.I membri del Comitato, previa designazione del rispettivo ente, istituzione o associazione rappresentativa, sono nominati con decreto del Presidente della Giunta regionale. La presidenza del Comitato spetta al Presidente della Giunta regionale o ad un suo delegato.
5.Il Presidente può, se richiesto, disporre la partecipazione, di volta in volta, di ulteriori soggetti tra quelli compresi all'articolo 2, commi 3 e 4, qualora dalla richiesta emerga un interesse concreto rispetto alle tematiche da trattare.
6.Il Comitato può avvalersi della consulenza della Commissione scientifica di valutazione di cui all'articolo 5.

Art. 5
(Commissione scientifica di valutazione)

1.Entro 180 giorni dalla entrata in vigore della presente legge la Giunta regionale, con proprio provvedimento, istituisce la Commissione scientifica di valutazione con la nomina di cinque componenti scelti tra i docenti universitari e le personalità di alta qualificazione scientifica, sulla base dei curricula presentati, in modo tale da assicurare la presenza di esperti nelle diverse discipline scientifiche.
2.Dura in carica per cinque anni ed elegge al suo interno un presidente. Può avvalersi di esperti esterni, anche internazionali, nelle specifiche materie oggetto della valutazione.
3.La Commissione è organo di consulenza della Regione Piemonte per la valutazione, anche in via preventiva, delle ricadute rispetto alle iniziative realizzate in attuazione delle linee generali di intervento di cui all'articolo 3. La Commissione valuta, altresì, i risultati delle iniziative realizzate in attuazione delle medesime linee.
4.La Commissione svolge funzioni di vigilanza sull'effettivo perseguimento degli obiettivi di cui all'articolo 1, comma 2, lettera i).
5.La Commissione presenta alla Giunta regionale entro il 31 marzo di ogni anno una relazione sulla attività svolta e sulle proposte formulate nell'anno solare precedente.
6.Ai componenti della Commissione spettano i compensi determinati dalla Giunta regionale con apposito provvedimento, in deroga alle disposizioni di cui alla legge regionale 2 luglio 1976, n. 33 (Compensi ai componenti Commissioni, Consigli, Comitati e Collegi operanti presso l'Amministrazione regionale).
7.Ulteriori criteri e modalità relativi all'organizzazione ed al funzionamento della Commissione scientifica di valutazione sono stabiliti nel provvedimento della Giunta regionale, di cui al comma 6.

Art. 6
(Coordinamento sulla ricerca)

1.Allo scopo di favorire una corretta circolazione delle informazioni e dei dati trattati all'interno della Regione e di garantirne una adeguata diffusione presso gli enti e le istituzioni interessati alla loro raccolta o elaborazione la Giunta regionale, con proprio provvedimento, istituisce il coordinamento delle direzioni regionali in materia di ricerca.
2.Con il provvedimento di cui al comma 1 la Giunta attribuisce, tra l'altro, le funzioni:
a)di segreteria e di supporto per il Comitato per la ricerca e l'innovazione previsto dall'articolo 4 e per la Commissione scientifica di valutazione prevista dall'articolo 5;

b)di raccolta ed aggiornamento, in una apposita banca dati informatizzata, delle principali informazioni sul Sistema Regionale della Ricerca.

Art. 7
(Norma finanziaria)

1.Per la attuazione della presente legge è autorizzata la spesa di euro 6.000.000,00 per il 2004 e di euro 7.000.000,00 per ciascuno degli anni 2005 e 2006.
2.A tal fine si provvede mediante l'istituzione di una nuova unità previsionale di base (UPB), denominata "Fondo integrativo per la promozione del Sistema regionale della ricerca" e collocata nel bilancio di previsione per l'anno finanziario 2004, all'interno della direzione Programmazione e statistica e corrispondente al Settore di cui all'articolo 6, comma 3.
3.Nello stato di previsione della spesa del bilancio 2004, nell'UPB di cui al 2 comma, sono previsti gli stanziamenti inerenti alle seguenti spese: "Spese per il funzionamento del Comitato per la ricerca e l'innovazione", "Spese per il funzionamento della Commissione scientifica di valutazione", "Spese per la selezione di progetti e programmi finanziati dal Piano pluriennale della ricerca", "Contributi per progetti e programmi finanziati dal Piano pluriennale della ricerca".
4.Agli oneri derivanti dalla applicazione della presente legge si provvede riducendo di euro 6.000.000,00 in termini di competenza e di cassa, la dotazione della UPB n. 16032 (Industria - Promozione e sviluppo delle P.M.I - Titolo II - Spese d'investimento), capitolo 26720, dello stato di previsione della spesa del bilancio di previsione per l'anno finanziario 2004.
5.Agli oneri quantificati per l'anno finanziario 2005 in euro 7.000.000,00, e per l'anno finanziario 2006 in euro 7.000.000,00 si provvede con le dotazioni della UPB 09011 (Bilanci e finanze - Bilanci - Titolo I - Spese correnti) del bilancio pluriennale 2004- 2006.

Art. 8
(Notifica delle azioni configurabili come aiuti di Stato)

1.Gli atti emanati in applicazione della presente legge che prevedano l'attivazione di azioni configurabili come aiuti di Stato, ad eccezione dei casi in cui detti aiuti siano erogati in conformità a quanto previsto dai regolamenti comunitari d'esenzione, sono oggetto di notifica ai sensi degli articoli 87 e 88 del Trattato.

Istituito con decreto legislativo il sistema pubblico di connettività - SPC per l'interconnessione informatica tra tutti gli uffici della p.a.

NUMERO SCHEDA: 6238

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

NATURA ATTO: DECRETO LEGISLATIVO

DATA ATTO: 28/02/2005

NUM. ATTO: 42

Nella seduta dell'11 febbraio 2005 il Consiglio dei ministri ha approvato in via definitiva, su proposta del Ministro per l'Innovazione e le Tecnologie e dei Ministri per la Funzione Pubblica, degli Esteri e dell'Economia e Finanze, il decreto legislativo che istituisce e regola il Sistema Pubblico di Connettività - SPC e la Rete Internazionale della Pubblica

Amministrazione. Il progetto SPC, considerato una sorta di enorme 'Autostrada del Sole digitale, costituisce un sistema di infrastrutture tecnologiche immateriali e di regole tecniche per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della PA, centrale e locale, che consente l'interconnessione tra tutti gli uffici pubblici per lo svolgimento in via informatica dei procedimenti amministrativi, i quali avranno validità giuridica. Tale collegamento informatico consentirà la comunicazione fra non meno di 15 mila uffici per l'erogazione di servizi resi in via telematica, sulla base dei più elevati standard tecnologici, organizzativi e di sicurezza.
Il Sistema, che dà attuazione alla previsione contenuta nell'art. 10 della legge 29 luglio 2003 n. 229 circa il riassetto in materia di società dell'informazione, costituisce il presupposto per l'applicazione del Codice dell'Amministrazione Digitale e rappresenta, inoltre, la base italiana della futura Rete Internazionale, infrastruttura transnazionale in grado di collegare oltre 500 uffici (ambasciate, consolati, uffici Ice, Camere di Commercio, Istituti Italiani di Cultura) in oltre 120 Paesi.
La creazione di una autostrada digitale, oltre a favorire un rapido accesso da parte di imprese e cittadini italiani, in patria e all'estero, ai servizi erogati dalla pubblica amministrazione, si prefigge di assicurare maggiore efficienza all'azione amministrativa e di ridurne sensibilmente i costi, realizzando un risparmio di almeno il 30% dei tempi di svolgimento dei provvedimenti fra amministrazioni e concretizzando una riduzione del 35% dei soli costi per le telecomunicazioni.
Le regole tecniche e di sicurezza per il funzionamento della nuova infrastruttura saranno fissate da un successivo decreto da emanarsi entro nove mesi dall'entrata in vigore del d.lgs in esame.
Al Centro nazionale per l'informatica nella pubblica amministrazione (Cnipa) spetterà il compito sia di occuparsi della progettazione, realizzazione ed evoluzione del sistema sia di gestire le risorse condivise. Presso il Cnipa sarà inoltre istituito l'elenco nazionale delle imprese fornitrici del sistema SPC; gli elenchi regionali saranno invece tenuti dalle singole regioni.
Per la realizzazione del SPC (è da sottolineare l'obbligo di migrazione dal sistema di connessione alla Rupa al nuovo sistema) è altresì prevista la stipulazione di contratti quadro a livello nazionale e regionale che stabiliranno condizioni e vincoli che i fornitori saranno tenuti a rispettare per la definizione dei contratti con le singole p.a..

Si riporta il testo del decreto legislativo n. 42 del 28 febbraio 2005 istitutivo del Sistema pubblico di connettività, pubblicato sulla G.U n. 73 del 30 marzo e in vigore dal 14 aprile 2005.

DECRETO LEGISLATIVO 28 febbraio 2005, n.42
Istituzione del sistema pubblico di connettività e della rete internazionale della pubblica amministrazione, a norma dell'articolo 10, della legge 29 luglio 2003, n. 229.

Capo I

Principi generali

Art. 1.
Definizioni

1. Ai fini del presente decreto si intende per:

a) «documento informatico»: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

b) «trasporto di dati»: i servizi per la realizzazione, gestione ed evoluzione di reti informatiche per la trasmissione di dati, oggetti multimediali e fonia;

c) «interoperabilità di base»: i servizi per la realizzazione, gestione ed evoluzione di strumenti per lo scambio di documenti informatici fra le pubbliche amministrazioni e tra queste e i cittadini;

d) «connettivita»: l'insieme dei servizi di trasporto di dati e di interoperabilita' di base;

e) «interoperabilita' evoluta»: i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini;

f) «cooperazione applicativa»: la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione delle informazioni e dei procedimenti amministrativi.

Art. 2.
Sistema pubblico di connettività

1. Nel rispetto dell'articolo 117, secondo comma, lettera r), della Costituzione, e nel rispetto dell'autonomia dell'organizzazione interna delle funzioni informative delle regioni e delle autonomie locali il presente decreto definisce e disciplina il sistema pubblico di connettività, di seguito «SPC», al fine di assicurare il coordinamento informativo e informatico dei dati tra le amministrazioni centrali, regionali e locali e promuovere l'omogeneita' nella elaborazione e trasmissione dei dati stessi, finalizzata allo scambio e diffusione delle informazioni tra le pubbliche amministrazioni e alla realizzazione di servizi integrati.

2. Il SPC è l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilita' di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.

3. La realizzazione del SPC avviene nel rispetto dei seguenti principi:

sviluppo architetturale ed organizzativo atto a garantire la natura federata, policentrica e non gerarchica del sistema;

b) economicita' nell'utilizzo dei servizi di rete, di interoperabilità e di supporto alla cooperazione applicativa;

c) sviluppo del mercato e della concorrenza nel settore delle tecnologie dell'informazione e della comunicazione.

Art. 3.
Rete internazionale delle pubbliche amministrazioni

1. Il presente decreto definisce e disciplina la Rete internazionale delle pubbliche amministrazioni, interconnessa al SPC.

La Rete costituisce l'infrastruttura di connettività che collega, nel rispetto della normativa vigente, le pubbliche amministrazioni con gli uffici italiani all'estero, garantendo adeguati livelli di sicurezza e qualita'.

Capo II
Sistema pubblico di connettività

Art. 4.
Partecipazione al Sistema pubblico di connettività

1. Al SPC partecipano tutte le amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165.

2. Il comma 1 non si applica alle amministrazioni di cui al decreto legislativo 30 marzo 2001, n. 165, limitatamente all'esercizio delle sole funzioni di ordine e sicurezza pubblica, difesa nazionale, consultazioni elettorali.

3. Ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 11 novembre 1994, n. 680, nonché dell'articolo 25 del decreto legislativo 30 giugno 2003, n. 196, è comunque garantita la connessione con il SPC dei sistemi informativi degli organismi competenti per l'esercizio delle funzioni di sicurezza e difesa nazionale, nel loro esclusivo interesse e secondo regole tecniche che assicurino riservatezza e sicurezza.

È altresi' garantita la possibilita' di connessione al SPC delle autorita' amministrative indipendenti.

Art. 5.
Scambio di documenti informatici nell'ambito del Sistema pubblico di connettività

1. Gli scambi di documenti informatici tra le pubbliche amministrazioni nell'ambito del SPC, avvengono nel rispetto delle procedure di cooperazione applicativa finalizzate allo svolgimento di procedimenti amministrativi e costituiscono invio documentale valido ad ogni effetto di legge se realizzate nel rispetto delle regole tecniche e di sicurezza di cui all'articolo 16.

Art. 6.
Finalita' del Sistema pubblico di connettività

1. Al SPC sono attribuite le seguenti finalita':

a) fornire un insieme di servizi di connettività condivisi dalle pubbliche amministrazioni interconnesse, definiti negli aspetti di funzionalita', qualita' e sicurezza, ampiamente graduabili in modo da poter soddisfare le differenti esigenze delle pubbliche amministrazioni aderenti al SPC;

b) garantire l'interazione della pubblica amministrazione centrale e locale con tutti gli altri soggetti connessi a Internet, nonché con le reti di altri enti, promuovendo l'erogazione di servizi di qualita' e la miglior fruibilita' degli stessi da parte dei cittadini e delle imprese;

c) fornire un'infrastruttura condivisa di interscambio che consenta l'interoperabilita' tra tutte le reti delle pubbliche amministrazioni esistenti, favorendone lo sviluppo omogeneo su tutto il territorio nella salvaguardia degli investimenti effettuati;

d) fornire servizi di connettività e cooperazione alle pubbliche amministrazioni che ne facciano richiesta, per permettere l'interconnessione delle proprie sedi e realizzare cosi' anche l'infrastruttura interna di comunicazione;

e) realizzare un modello di fornitura dei servizi multifornitore coerente con l'attuale situazione di mercato e le dimensioni del progetto stesso;

f) garantire lo sviluppo dei sistemi informatici nell'ambito del SPC salvaguardando la sicurezza dei dati, la riservatezza delle informazioni, nel rispetto dell'autonomia del patrimonio informativo delle singole amministrazioni e delle vigenti disposizioni in materia di protezione dei dati personali.

Art. 7.
Compiti delle pubbliche amministrazioni nel Sistema pubblico di connettività

1. Le pubbliche amministrazioni nell'ambito della loro autonomia funzionale e gestionale adottano nella progettazione e gestione dei propri sistemi informativi, ivi inclusi gli aspetti organizzativi, soluzioni tecniche compatibili con la cooperazione applicativa con le altre pubbliche amministrazioni, secondo le regole tecniche di cui all'articolo 16.

2. Per le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, le responsabilita' di cui al comma 1 sono attribuite al dirigente responsabile dei sistemi informativi automatizzati, di cui all'articolo 10, comma 1, dello stesso decreto legislativo.

Art. 8.
Commissione di coordinamento del Sistema pubblico di connettività

1. È istituita la Commissione di coordinamento del SPC, di seguito denominata: «Commissione», preposta agli indirizzi strategici del SPC.
2. La Commissione:
a) assicura il raccordo tra le amministrazioni pubbliche, nel rispetto delle funzioni e dei compiti spettanti a ciascuna di esse;
b) approva le linee guida, le modalita' operative e di funzionamento dei servizi e delle procedure per realizzare la cooperazione applicativa fra i servizi erogati dalle amministrazioni;
c) promuove l'evoluzione del modello organizzativo e dell'architettura tecnologica del SPC in funzione del mutamento delle esigenze delle pubbliche amministrazioni e delle opportunita' derivanti dalla evoluzione delle tecnologie;
d) promuove la cooperazione applicativa fra le pubbliche amministrazioni, nel rispetto delle regole tecniche di cui all'articolo 16;
e) definisce i criteri e ne verifica l'applicazione in merito alla iscrizione, sospensione e cancellazione dagli elenchi dei fornitori qualificati SPC di cui all'articolo 11;
f) dispone la sospensione e cancellazione dagli elenchi dei fornitori qualificati di cui all'articolo 11;
g) verifica la qualita' e la sicurezza dei servizi erogati dai fornitori qualificati del SPC;
h) promuove il recepimento degli standard necessari a garantire la connettività, l'interoperabilita' di base e avanzata, la cooperazione applicativa e la sicurezza del Sistema.
3. Le decisioni della Commissione sono assunte a maggioranza semplice o qualificata dei componenti in relazione all'argomento in esame. La Commissione a tale fine elabora, entro tre mesi dal suo insediamento, un regolamento interno da approvare con maggioranza qualificata dei suoi componenti.

Art. 9.
Composizione della Commissione di coordinamento del Sistema pubblico di connettività

1. La Commissione è formata da tredici componenti incluso il Presidente di cui al comma 2, scelti tra persone di comprovata professionalita' ed esperienza nel settore, nominati con decreto del Presidente del Consiglio dei Ministri, sei in rappresentanza delle amministrazioni statali previa deliberazione del Consiglio dei Ministri, su proposta del Ministro per l'innovazione e le tecnologie ed i restanti sei su designazione della Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281. Quando esamina questioni di interesse della rete internazionale della pubblica amministrazione, la Commissione è integrata da un rappresentante del Ministero degli affari esteri.
2. Il Presidente del Centro nazionale per l'informatica nella pubblica amministrazione, è componente di diritto e presiede la Commissione. Gli altri componenti della Commissione restano in carica per un biennio e l'incarico è rinnovabile.
3. La Commissione è convocata dal Presidente e si riunisce almeno quattro volte l'anno.
4. L'incarico di Presidente o di componente della Commissione e la partecipazione alle riunioni della Commissione non danno luogo a compensi e gli eventuali oneri di missione sono a carico delle amministrazioni di appartenenza.
5. Per i necessari compiti istruttori la Commissione si avvale del Centro nazionale per l'informatica nella pubblica amministrazione, di seguito denominato: «CNIPA» e sulla base di specifiche convenzioni, di organismi interregionali e territoriali.
6. La Commissione puo' avvalersi, senza alcun aggravio di spesa, della consulenza di uno o più organismi di consultazione e cooperazione istituiti con appositi accordi ai sensi dell'articolo 9, comma 2, lettera c), del decreto legislativo 28 agosto 1997, n. 281.

7. Ai fini della definizione degli sviluppi strategici del SPC, in relazione all'evoluzione delle tecnologie dell'informatica e della comunicazione, la Commissione puo' avvalersi di consulenti di chiara fama ed esperienza in numero non superiore a cinque secondo le modalita' definite nei regolamenti di cui all'articolo 17. I relativi costi sono a carico del CNIPA.

Art. 10.
Ruolo del Centro nazionale per l'informatica nella pubblica amministrazione

1. Il CNIPA, nel rispetto delle decisioni e degli indirizzi forniti dalla Commissione, anche avvalendosi di soggetti terzi, gestisce le risorse condivise del SPC e le strutture operative preposte al controllo e supervisione delle stesse, per tutte le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165.
2. Il CNIPA, anche avvalendosi di soggetti terzi, cura la progettazione, la realizzazione, la gestione e l'evoluzione del SPC per le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39.

Art. 11.
Fornitori del Sistema pubblico di connettività

1. Sono istituiti uno o più elenchi di fornitori a livello nazionale e regionale in attuazione delle finalita' di cui all'articolo 6.
2. I fornitori che ottengono la qualificazione SPC ai sensi dei regolamenti previsti dall'articolo 17, sono inseriti negli elenchi di competenza nazionale o regionale, consultabili in via telematica, esclusivamente ai fini dell'applicazione della disciplina di cui al presente decreto, e tenuti rispettivamente dal CNIPA a livello nazionale e dalla regione di competenza a livello regionale. I fornitori in possesso dei suddetti requisiti sono denominati fornitori qualificati SPC.
3. I servizi per i quali è istituito un elenco, ai sensi del comma1, sono erogati, nell'ambito del SPC, esclusivamente dai soggetti che abbiano ottenuto l'iscrizione nell'elenco di competenza nazionale o regionale.
4. Per l'iscrizione negli elenchi dei fornitori qualificati SPC è necessario che il fornitore soddisfi almeno i seguenti requisiti:
a) disponibilità di adeguate infrastrutture e servizi di comunicazioni elettroniche;
b) esperienza comprovata nell'ambito della realizzazione gestione ed evoluzione delle soluzioni di sicurezza informatica;
c) possesso di adeguata rete commerciale e di assistenza tecnica;
d) possesso di adeguati requisiti finanziari e patrimoniali, anche dimostrabili per il tramite di garanzie rilasciate da terzi qualificati.
5. Limitatamente ai fornitori dei servizi di connettività dovranno inoltre essere soddisfatti anche i seguenti requisiti:
a) possesso dei necessari titoli abilitativi di cui al decreto legislativo 1° agosto 2003, n. 259, per l'ambito territoriale di esercizio dell'attivita';
b) possesso di comprovate conoscenze ed esperienze tecniche nella gestione delle reti e servizi di comunicazioni elettroniche, anche sotto il profilo della sicurezza e della protezione dei dati.

Art. 12.
Contratti quadro

1. Al fine della realizzazione del SPC, il CNIPA a livello nazionale e le regioni nell'ambito del proprio territorio, per soddisfare esigenze di coordinamento, qualificata competenza e indipendenza di giudizio, nonché per garantire la fruizione, da parte delle pubbliche amministrazioni, di elevati livelli di disponibilità dei servizi e delle stesse condizioni contrattuali proposte dal miglior offerente, nonché

una maggiore affidabilita' complessiva del sistema, promuovendo, altresi', lo sviluppo della concorrenza e assicurando la presenza di più fornitori qualificati, stipulano, espletando specifiche procedure ad evidenza pubblica per la selezione dei contraenti, nel rispetto delle vigenti norme in materia, uno o più contratti-quadro con più fornitori per i servizi di cui all'articolo 6, con cui i fornitori si impegnano a contrarre con le singole amministrazioni alle condizioni ivi stabilite.

2. Le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, sono tenute a stipulare gli atti esecutivi dei contratti-quadro con uno o più fornitori di cui al comma 1, individuati dal CNIPA. Gli atti esecutivi non sono soggetti al parere del CNIPA e, ove previsto, del Consiglio di Stato. Le amministrazioni non ricomprese tra quelle di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, hanno facoltà di stipulare gli atti esecutivi di cui al presente articolo.

Art. 13.
Migrazione della Rete unitaria della pubblica amministrazione

1. Le Amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, aderenti alla Rete unitaria della pubblica amministrazione, presentano al CNIPA, secondo le indicazioni da esso fornite, entro sei mesi dalla data di entrata in vigore del presente decreto, i piani di migrazione verso il SPC, da attuarsi entro diciotto mesi dalla data di approvazione del primo contratto quadro di cui all'articolo 12, comma 1, termine di cessazione dell'operativita' della Rete unitaria della pubblica amministrazione, e comunque non oltre trenta mesi dalla medesima data di entrata in vigore del presente decreto.

2. Trascorsi trenta mesi dalla data di entrata in vigore del presente decreto ogni riferimento normativo alla Rete unitaria della pubblica amministrazione si intende effettuato al SPC.

Capo III

Rete internazionale della pubblica amministrazione

Art. 14.
Collegamenti operanti per il tramite della Rete internazionale delle pubbliche amministrazioni

1. Le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, che abbiano l'esigenza di connettività verso l'estero, sono tenute ad avvalersi dei servizi offerti dalla Rete internazionale delle pubbliche amministrazioni, interconnessa al SPC.

2. Le pubbliche amministrazioni di cui al comma 1, che dispongono di reti in ambito internazionale sono tenute a migrare nella Rete internazionale delle pubbliche amministrazioni entro e non oltre due anni a decorrere dalla data di entrata in vigore del presente decreto, fatto salvo quanto previsto dall'articolo 4, commi 2 e 3.

3. Le amministrazioni non ricomprese tra quelle di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, ivi incluse le autorita' amministrative indipendenti, possono aderire alla Rete internazionale delle pubbliche amministrazioni.

Art. 15.
Compiti del CNIPA

1. Il CNIPA cura la progettazione, la realizzazione, la gestione ed evoluzione della Rete internazionale delle pubbliche amministrazioni, previo espletamento di procedure concorsuali ad evidenza pubblica per la selezione dei fornitori e mediante la stipula di appositi contratti-quadro secondo modalita' analoghe a quelle di cui all'articolo 12.

Capo IV

Art. 16.

Regole tecniche

1. Entro nove mesi dalla data di entrata in vigore del presente decreto, con uno o più decreti, adottati sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, sono adottate le regole tecniche e di sicurezza per il funzionamento del SPC.

Art. 17.

Regolamenti

1. Ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, con uno o più decreti sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, sono adottati regolamenti per l'organizzazione del SPC e della Commissione di cui all'articolo 9, per l'avvalimento dei consulenti di cui all'articolo 9, comma 7, e per la determinazione dei livelli minimi dei requisiti richiesti per l'iscrizione agli elenchi dei fornitori qualificati del SPC di cui all'articolo 11.

Art. 18.

Disposizioni finali

1. Il CNIPA, al fine di favorire una rapida realizzazione del SPC, per un periodo almeno pari a due anni a decorrere dalla data di approvazione dei contratti-quadro di cui all'articolo 12, comma 1, sostiene i costi delle infrastrutture condivise, a valere sulle risorse gia' previste nel bilancio dello Stato.

2. Al termine del periodo di cui al comma 1 i costi relativi alle infrastrutture condivise sono a carico dei fornitori proporzionalmente agli importi dei contratti di fornitura, e una quota di tali costi è a carico delle pubbliche amministrazioni relativamente ai servizi da esse utilizzati. I costi, i criteri e la relativa ripartizione tra le amministrazioni sono determinati annualmente con decreto del Presidente del Consiglio dei Ministri, su proposta della Commissione, previa intesa con la Conferenza unificata cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, salvaguardando eventuali intese locali finalizzate a favorire il pieno ingresso nel SPC dei piccoli Comuni nel rispetto di quanto previsto dal comma 5.

3. Il CNIPA sostiene tutti gli oneri derivanti dai collegamenti in ambito internazionale delle amministrazioni di cui all'articolo 14, comma 1, per i primi due anni di vigenza contrattuale, decorrenti dalla data di approvazione del contratto quadro di cui all'articolo 12; per gli anni successivi ogni onere è a carico della singola amministrazione contraente proporzionalmente ai servizi acquisiti.

4. Le amministrazioni non ricomprese tra quelle di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, che aderiscono alla Rete internazionale delle pubbliche amministrazioni, ai sensi dell'articolo 14, comma 3, ne sostengono gli oneri relativi ai servizi che utilizzano.

5. Le disposizioni del presente decreto si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

6. Dall'attuazione del presente decreto non derivano nuovi o maggiori oneri a carico della finanza pubblica.

Art. 19.
Abrogazioni

1. L'articolo 15, comma 1, della legge 15 marzo 1997, n. 59, è abrogato trascorsi trenta mesi dalla data di entrata in vigore del presente decreto.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addi' 28 febbraio 2005

Un articolo sull'informatizzazione dell'attività amministrativa nella giurisprudenza e nella prassi.

NUMERO SCHEDA: 6196

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: GIORNALE DI DIRITTO AMMINISTRATIVO

AUTORE: Angelo Giuseppe Orfino

NUMERO: 12

DATA: 31/12/2004

PAGINA: 1371-1382

RIFERIMENTO NORMATIVO:

NATURA ATTO: COMMENTO

E' un articolo, a cura di Angelo Giuseppe Orfino, concernente "L'informatizzazione dell'attività amministrativa nella giurisprudenza e nella prassi", molto ricco di riferimenti legislativi, giurisprudeniali e dottrinali.

Il commento evidenzia come l'uso degli strumenti informatici e telematici stia modificando il modo di svolgimento dell'attività amministrativa, ponendo conseguentemente nuove problematiche, sia di carattere giuridico, che tecnico e organizzativo, legate alle peculiarità del mezzo usato.

Nell'articolo l'autore, attraverso l'esame della giurisprudenza nonché di taluni casi concreti, offre una panoramica su alcune delle questioni di maggiore interesse in materia di informatizzazione dell'attività amministrativa.

L'articolo si articola nelle seguenti parti.

Il commento è in visione presso il settore Studi e documentazione legislativi.

- Premessa.
- L'automazione amministrativa.
- L'attività in forma elettronica.
- La pubblicazione di atti amministrativi in Rete.

- La comunicazione individuale via e-mail.

Una circolare del Ministero dell'Interno fornisce le prime indicazioni operative sulla carta d'identità elettronica.

NUMERO SCHEDA: 6164

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: ITALIA OGGI

AUTORE: S. Manzelli

DATA: 26/04/2005

PAGINA: 23

RIFERIMENTO NORMATIVO: l. 43/2005

NATURA ATTO: CIRCOLARE

DATA ATTO: 18/04/2005

NUM. ATTO: 20

ORGANO: MINISTERI

In data 18 aprile 2005 il ministero dell'Interno (dipartimento per gli Affari interni e territoriali, direzione centrale per i Servizi demografici) ha emesso la circolare n. 20 avente ad oggetto "Carta d'identità elettronica - Disposizioni innovative - Legge 31/3/2005 n. 43 di conversione, con modificazioni, del decreto legge 31 gennaio 2005, n. 7".
La legge n. 43/2005, alla quale la circolare fa riferimento, ha previsto che, a partire dal 1 gennaio 2006, a tutti coloro che ne facciano richiesta, venga rilasciata la carta d'identità elettronica in luogo della tradizionale carta d'identità cartacea.
A tal fine questa legge pone a carico dei comuni l'obbligo di provvedere, entro il 31 ottobre 2005, alla predisposizione dei necessari collegamenti all'Indice nazionale delle anagrafi e alla redazione del piano di sicurezza per la gestione delle postazioni di emissione.
La circolare, nel fornire le prime indicazioni operative alle prefetture, invita alla sensibilizzazione dei sindaci sulla necessità di identificare ed assegnare le risorse umane predisposte al rilascio di tale documento e ad adottare tutte le misure necessarie per conseguire le finalità sancite dalla legge n. 43/2005.
Le prefetture dovranno assicurare una costante ed efficace attività di monitoraggio e controllo sulle attività svolte e sulle iniziative assunte dai comuni.
La circolare informa altresì che è in corso di predisposizione un progetto di informatizzazione della gestione delle carte d'identità cartacee.
Si allega il testo della circolare.

Si segnala un commento in materia di carta d'identità elettronica, a cura di Paolo Subioli, sulla rivista "Guida agli Enti Locali", n. 21 del 28 maggio 2005, pp. 79-81, consultabile presso il settore Studi e documentazione legislativi.

Ministero dell'Interno
Dipartimento per gli Affari Interni e Territoriali
Direzione Centrale per i Servizi Demografici
Prot. n 200503670/15100/15850
Roma, 18 aprile 2005

CIRCOLARE N. 20 /2005
Oggetto: Carta d' identità elettronica - Disposizioni innovative - Legge 31 /3/ 2005 n. 43 di conversione , con modificazioni, del decreto legge 31 gennaio 2005, n. 7.
Con la legge 31.3.2005 n. 43, pubblicata sulla Gazzetta Ufficiale ,Serie generale n. 75 del 1.4.2005 è stato convertito in legge il decreto-legge 31 gennaio 2005, n. 7, recante disposizioni urgenti per l'università e la ricerca, per i beni e le attività culturali, per il completamento di grandi opere strategiche, per la mobilità dei pubblici dipendenti, nonché per semplificare gli adempimenti relativi a imposte di bollo e tasse di concessione. Sanatoria degli effetti dell'art.4, comma 1, del decreto legge 29 novembre 2004, n. 280.
L'art. 7-vicies ter comma 2 della citata legge dispone che, a decorrere dal 1.1.2006, venga rilasciata la carta d'identità elettronica, in luogo della carta d'identità su supporto cartaceo, a coloro che ne facciano richiesta (primo rilascio o rinnovo).
A tal fine la norma pone a carico dei Comuni l'obbligo di provvedere, entro il 31.10.2005, alla predisposizione dei necessari collegamenti all'Indice Nazionale delle anagrafi (INA) presso il Centro Nazionale per i servizi demografici (CNSD) e alla redazione del piano di sicurezza per la gestione delle postazioni di emissione, secondo le regole tecniche fornite dal Ministero dell'Interno.
Questa Direzione Centrale sta predisponendo una serie di iniziative necessarie per la realizzazione di un efficace modello di emissione della carta d'identità, nel rispetto dei termini indicati nella citata disposizione legislativa.
Nel richiamare la Direttiva del Ministro dell'Interno per l'anno 2005, nella quale vengono evidenziate le priorità politiche e gli obbiettivi dell'azione amministrativa, si invitano le SS.LL. a voler sensibilizzare opportunamente i signori Sindaci sulla necessità di identificare e assegnare, preferibilmente nell'ambito degli operatori demografici, le risorse umane che dovranno essere applicate, con stabilità, al rilascio dei documenti, nonché di definire le infrastrutture tecniche necessarie e di adottare tutti i provvedimenti indispensabili per conseguire le finalità sancite dalla citata legge (es. aggiornamento INA-SAIA).
Le SS.LL. dovranno, altresì, assicurare lo svolgimento di un efficace e costante attività di monitoraggio e controllo sulle attività svolte e sulle iniziative assunte dai Comuni, avvalendosi, a tal fine, del nuovo modello informatizzato di vigilanza anagrafica, reperibile sul sito "www.servizidemografici.interno.it", oggetto della circolare Min. Interno n. 57 (2004) del 25.11.2004, nella quale si è sottolineata l'importanza che riveste l'attività di vigilanza anagrafica, per la concreta realizzazione dei progetti di innovazione intrapresi dal Ministero dell'Interno nella materia demografica.
Si informano, inoltre, le SS.LL. che è in corso di predisposizione un progetto di informatizzazione della gestione delle carte d'identità cartacee, attraverso la creazione di un sistema che vede coinvolti in prima linea codesti spettabili Uffici Territoriali del Governo e che consentirà, una volta collegato al circuito di rilascio delle CIE, di avere, in tempo reale, un'informazione completa e aggiornata su ogni singola carta d'identità prodotta dall'Istituto Poligrafico dello Stato, con il dichiarato intento di semplificare e ridurre gli adempimenti gravanti sulle Forze dell'ordine.
Si ringrazia per la proficua e fattiva collaborazione.
Si resta in attesa di ricevere assicurazione del ricevimento della presente, via fax o tramite e-mail, al seguente indirizzo di posta elettronica: mariagabriella.onorati@interno.it

La Corte Costituzionale si pronuncia sulle competenze dello stato e delle regioni in materia di innovazione tecnologica.

NUMERO SCHEDA: 6132

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: CORTE COSTITUZIONALE

RIFERIMENTO NORMATIVO: l. n. 289/2002; l. n. 3/2003

NATURA ATTO: SENTENZA

DATA ATTO: 26/01/2005

NUM. ATTO: 31

ORGANO: CORTE COSTITUZIONALE

SCHEDE COLLEGATE: 5720

Con sentenza n. 31 del 26 gennaio 2005 la Corte Costituzionale si è pronunciata su alcuni ricorsi della Regione Emilia Romagna aventi ad oggetto numerose disposizioni della legge 27 dicembre 2002, n. 289 (Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato - legge finanziaria 2003) e della legge 16 gennaio 2003, n. 3 (Disposizioni ordinamentali in materia di pubblica amministrazione), in relazioni alle quali la regione ricorrente ha dedotto la violazione degli articoli 117, 118 e 119 della Costituzione nonché del principio di leale collaborazione. La Corte ha dichiarato non fondate le questioni sollevate ed analizzate nella decisione ad eccezione di una, in relazione alla quale è stata dichiarata l'illegittimità costituzionale dell'art. 26, comma 3, della l. 289/2002 . La Corte si è pronunciata su alcune questioni che, per ragioni di omogeneità di materia (l'innovazione tecnologica), una volta riuniti i giudizi, hanno potuto essere decise con la medesima sentenza, separandole quindi da altre questioni proposte con i medesimi ricorsi. Sono state dichiarate non fondate le questioni relative alle seguenti disposizioni: - art. 26, commi 1, secondo periodo, della l. 289/2002. Tale articolo prevede l' istituzione di un «*Fondo per il finanziamento di progetti di innovazione tecnologica nelle pubbliche amministrazioni e nel Paese*», stabilendo che con decreti ministeriali «*di natura non regolamentare*» siano definite le modalità di funzionamento del Fondo stesso ed individuati «*i progetti da finanziare e, ove necessario, la relativa ripartizione tra le amministrazioni interessate* »; - art. 26, comma 2 della l. 289/2002, che attribuisce allo stesso Ministro per l'innovazione e le tecnologie – al fine di razionalizzare la spesa informatica, nonché di indirizzare gli investimenti nelle tecnologie informatiche – vari poteri di direttiva, controllo, coordinamento, valutazione, approvazione di piani e progetti. A giudizio della Corte, le funzioni connesse ai processi di informatizzazione della P.A. non

sono da ricondursi alla competenza residuale esclusiva regionale in materia di organizzazione amministrativa regionale e degli enti locali, bensì al "*coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale*" che, a norma dell'art. 117, 2 comma, lettera r) Cost.costituisce espressione della potestà legislativa esclusiva statale. - art. 56 della l. n. 289/2002.Questo articolo istituisce un fondo finalizzato al finanziamento di progetti di ricerca di rilevante valore scientifico, anche con riguardo alla tutela della salute e dell'innovazione tecnologica, alla ripartizione del quale provvede il Presidente Consiglio dei Ministri con decreto nel quale sono altresì stabiliti procedure, modalità e strumenti per l'utilizzo delle risorse. Secondo la ricorrente tale disposizione – istituendo un «*Fondo settoriale a gestione centrale*» e attribuendo con norme di dettaglio «*poteri sostanzialmente normativi ed amministrativi al Presidente del Consiglio dei Ministri*» – violerebbe gli artt. 117, terzo e sesto comma, 118, secondo comma, e 119 della Costituzione. La Corte dichiara non fondata la questione rinviando alle motivazioni della sentenza n. 423/2004 (v. scheda n. 5720) la quale ha affermato che la ricerca scientifica deve essere considerata non solo una "*materia*", ma anche un "*valore*" costituzionalmente protetto (artt. 9 e 33 della Costituzione), in quanto tale in grado di rilevare a prescindere da ambiti di competenze rigorosamente delimitati. Sulla base di tale premesse la sentenza citata legittima un intervento statale particolarmente ampio in materia. - art. 27 della l. , comma 8, della l. n. 3/2003. Tale norma prevede l'emanazione a livello governativo di una serie di regolamenti finalizzati a realizzare alcune misure a garanzia dell'innovazione tecnologica (estensione dell'uso della posta elettronica nella P.A., alfabetizzazione informatica dei dipendenti, ecc.). La Corte ritiene che tale disposizione non incida, come sostenuto dalla ricorrente, sulla materia dell'organizzazione interna delle regioni e degli enti locali, in quanto i contenuti della norma stessa vanno riferiti esclusivamente all'amministrazione statale. - La Corte ha invece dichiarato fondata la questione relativa all' art. 26, comma 3 della l. 289/2002, la quale prevede che «nei casi in cui i progetti di cui ai commi 1 e 2 riguardino l'organizzazione e la dotazione tecnologica delle Regioni e degli enti territoriali, i provvedimenti sono adottati sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281»- Tale disposizione è stata dichiarata illegittima in quanto la previsione del semplice parere della Conferenza unificata non costituisce, nel caso di specie, una misura adeguata a garantire il rispetto del principio di leale collaborazione. Non è sufficiente, a giudizio della Corte, un semplice parere della Conferenza unificata: solo lo strumento dell'intesa garantisce un più incisivo coinvolgimento delle regioni e degli enti locali. Si allega il testo della sentenza.

Si segnala un commento alla sentenza, sulla rivista federalismi.it, n. 5/2005, a cura di Valerio Sarcone, intitolato "La Leale collaborazione vale anche per l'e-government? Dalla Consulta un'occasione per trattare dell'innovazione tecnologica nelle amministrazioni (Brevissime considerazioni a margine della sent. Corte Cost., 26 gennaio 2005, n. 31)", consultabile presso il settore Studi e documentazione legislativi.

SENTENZA N. 31 ANNO 2005
LA CORTE COSTITUZIONALE

Ritenuto in fatto

1.— La Regione Emilia-Romagna, con ricorso (reg. ric. n. 25 del 2003) notificato il 1° marzo 2003 e depositato il successivo giorno 7, ha impugnato diverse disposizioni della legge 27 dicembre 2002, n. 289 (Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato – legge finanziaria 2003), tra cui l'art. 26, commi 1, secondo periodo, 2 e 3, e l'art. 56, per violazione degli artt. 117, 118 e 119 della Costituzione, nonché del principio di leale collaborazione.

Il primo comma dell'art. 26 prevede la istituzione di un «Fondo per il finanziamento di progetti di innovazione tecnologica nelle pubbliche amministrazioni e nel Paese», stabilendo che il Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e il Ministro dell'economia e delle finanze, con decreti «di natura non regolamentare», definisca le modalità di funzionamento del Fondo stesso ed individui «i progetti da finanziare e, ove necessario, la relativa ripartizione tra le amministrazioni interessate».

Il secondo comma dello stesso art. 26 attribuisce allo stesso Ministro per l'innovazione e le tecnologie – al fine di razionalizzare la spesa informatica, nonché di indirizzare gli investimenti nelle tecnologie informatiche – vari poteri di direttiva, controllo, coordinamento, valutazione, approvazione di piani e progetti.

Il terzo comma, infine, prevede che «nei casi in cui i progetti di cui ai commi 1 e 2 riguardino l'organizzazione e la dotazione tecnologica delle Regioni e degli enti territoriali, i provvedimenti sono adottati sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281».

Secondo la ricorrente tale disciplina, nella parte in cui si applica «alle Regioni, agli enti pararegionali e agli enti locali», inciderebbe sull'"organizzazione amministrativa regionale e degli enti locali", materia rientrante nella competenza legislativa esclusiva delle Regioni. La gestione ministeriale di un fondo settoriale in tale materia sarebbe, pertanto, lesiva dell'autonomia finanziaria delle Regioni stesse, in quanto, in base ai principî di cui all'art. 119 della Costituzione, quest'ultime dovrebbero «poter gestire autonomamente le risorse nelle materie di propria competenza». Risulterebbero, altresì, lese le competenze legislative e amministrative regionali, atteso che la disposizione censurata conferirebbe al Ministro, con norme di dettaglio, «poteri sostanzialmente normativi ed amministrativi» in materia regionale. Né, prosegue la ricorrente, potrebbe ritenersi legittima la norma perché la stessa fa riferimento a decreti «di natura non regolamentare», in quanto si tratta di atti che, alla luce dei criteri sostanziali di identificazione, hanno valenza normativa, non essendo sufficiente l'utilizzo di una determinata «etichetta» perché l'atto stesso possa mutare natura.

Le suddette lesioni permarrebbero nonostante sia previsto dal terzo comma della norma censurata il parere della Conferenza unificata, atteso che il parere è un «mero strumento di partecipazione e per di più assai debole».

La ricorrente ritiene, infine, che la illegittimità costituzionale della norma permarrebbe anche qualora si intendesse ricondurre il contenuto della disposizione impugnata alla materia concorrente "sostegno all'innovazione per i settori produttivi", che «a dire il vero, sembra fare riferimento alle imprese e non alle pubbliche amministrazioni». Lo Stato si sarebbe, infatti, dovuto limitare a dettare i principî fondamentali e non anche norme di dettaglio, essendogli, altresì, precluso, in base a quanto statuito dall'art. 117, sesto comma, della Costituzione, emanare regolamenti statali, nonché allocare le funzioni amministrative *ex* art. 118 della Costituzione, in materie rientranti nella competenza legislativa concorrente.

In definitiva, la disposizione impugnata risulterebbe illegittima «nella parte in cui attribuisce al Ministro poteri normativi ed amministrativi relativi alla gestione del Fondo in questione anche in relazione alle Regioni, agli enti pararegionali e agli enti locali, anziché prevedere la mera ripartizione del Fondo tra le Regioni. In subordine, esso risulta illegittimo nella parte in cui non prevede che i poteri statali siano esercitati previa intesa con la Conferenza unificata, dato che nelle materie regionali il principio di leale collaborazione impone un coordinamento fra i soggetti interessati».

1.1.— Si è costituito il Presidente del Consiglio dei ministri, rappresentato e difeso dall'Avvocatura generale dello Stato, chiedendo che la questione venga dichiarata non fondata, non incidendo la norma su competenze riservate alle Regioni.

2.— Con lo stesso ricorso (reg. ric. n. 25 del 2003) la Regione Emilia-Romagna ha, altresì, impugnato l'art. 56 della medesima legge n. 289 del 2002, che ha «istituito un Fondo finalizzato al finanziamento di progetti di ricerca, di rilevante valore scientifico, anche con riguardo alla tutela della salute e all'innovazione tecnologica, con una dotazione finanziaria di 225 milioni di euro per l'anno 2003 e di 100 milioni di euro a decorrere dall'anno 2004»; stabilendo, altresì, che: alla «ripartizione del Fondo, istituito nello stato di previsione del Ministero dell'economia e delle finanze, tra le diverse finalità provvede il Presidente del Consiglio dei ministri, con proprio decreto, su proposta del Ministro dell'istruzione, dell'università e della ricerca, sentiti i Ministri dell'economia e delle finanze, della salute e per l'innovazione tecnologica. Con lo stesso decreto sono stabiliti procedure, modalità e strumenti per l'utilizzo delle risorse, assicurando in via prioritaria il finanziamento dei progetti presentati da soggetti che abbiano ottenuto, negli anni precedenti, un eccellente risultato nell'utilizzo e nella capacità di spesa delle risorse comunitarie assegnate e delle risorse finanziarie provenienti dai programmi quadro di ricerca dell'Unione europea o dai Fondi strutturali».

Secondo la ricorrente tale disposizione – istituendo un «Fondo settoriale a gestione centrale» e attribuendo con norme di dettaglio «poteri sostanzialmente normativi ed amministrativi al Presidente del Consiglio dei Ministri» – violerebbe gli artt. 117, terzo e sesto comma, 118, secondo comma, e 119 della Costituzione.

Anche in questo caso la Regione conclude affermando che la norma impugnata risulterebbe illegittima per la violazione tanto di sfere di competenza regionale, quanto del principio di leale collaborazione che impone un coordinamento fra i soggetti interessati.

2.1.— Si è costituito il Presidente del Consiglio dei ministri, rappresentato e difeso dall'Avvocatura generale dello Stato, chiedendo che la questione venga dichiarata non fondata, in quanto «da nessun principio costituzionale è lecito trarre la conclusione che non è consentito al legislatore statale prevedere la istituzione di un (…) Fondo settoriale – il che non incide né limita in alcun modo la sfera di competenza regionale – la cui gestione è coerentemente attribuita, anche per quanto riguarda l'utilizzo delle risorse, agli organi dello stesso Stato».

3.— La Regione Emilia-Romagna, con ricorso (reg. ric. n. 32 del 2003) notificato il 21 marzo 2003 e depositato il successivo giorno 27, ha impugnato diverse disposizioni della legge 16 gennaio 2003, n. 3 (Disposizioni ordinamentali in materia di pubblica amministrazione), tra cui, per quanto qui interessa, l'art. 27, comma 8, per violazione dell'art. 117, quarto comma, della Costituzione.

La norma censurata stabilisce che, entro un anno dalla data di entrata in vigore della suddetta legge, «sono emanati uno o più regolamenti, ai sensi dell'articolo 117, sesto comma, della Costituzione e dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, per introdurre nella disciplina vigente le norme necessarie ai fini del conseguimento dei seguenti obiettivi: a) diffusione dei servizi erogati in via telematica ai cittadini e alle imprese, anche con l'intervento dei privati, nel rispetto dei principi di cui all'articolo 97 della Costituzione e dei provvedimenti già adottati; b) diffusione e uso della carta nazionale dei servizi; c) diffusione dell'uso delle firme elettroniche; d) ricorso a procedure telematiche da parte della pubblica amministrazione per l'approvvigionamento di beni e servizi, potenziando i servizi forniti dal Ministero dell'economia e delle finanze attraverso la CONSIP Spa (Concessionaria servizi informativi pubblici); e) estensione dell'uso della posta elettronica nell'àmbito delle pubbliche amministrazioni e dei rapporti tra pubbliche amministrazioni e privati; f) generalizzazione del ricorso a procedure telematiche nella contabilità e nella tesoreria; g) alfabetizzazione informatica dei pubblici dipendenti; h) impiego della telematica nelle attività di formazione dei dipendenti pubblici; i) diritto di accesso e di reclamo esperibile in via telematica da parte dell'interessato nei confronti delle pubbliche amministrazioni».

Secondo la ricorrente la norma riportata inciderebbe – come dimostrerebbe la stessa rubrica recante "Disposizioni in materia di innovazione tecnologica nella pubblica amministrazione" – «essenzialmente sulla materia dell'organizzazione interna delle Regioni, degli enti locali e degli enti pubblici di carattere regionale», nonché sulla materia della formazione professionale [lettere *g*) e *h*) della disposizione impugnata]. In presenza, pertanto, di materie di competenza regionale sarebbe illegittima la previsione di un regolamento statale *ex* art. 117, sesto comma, della Costituzione, che «potrà valere per lo Stato e per gli

enti pubblici nazionali, mentre spetta alle Regioni la disciplina per le amministrazioni cui si riferisce la legislazione regionale».

3.1.— Si è costituito il Presidente del Consiglio dei ministri, rappresentato e difeso dall'Avvocatura generale dello Stato, chiedendo che la questione venga dichiarata non fondata, in quanto l'oggetto della disciplina della norma impugnata dovrebbe essere ricondotto alla materia "coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale" di competenza legislativa esclusiva statale *ex* art. 117, secondo comma, lettera *r*), della Costituzione.

4.— Nell'imminenza dell'udienza pubblica la Regione Emilia-Romagna ha depositato memorie in relazione ai ricorsi sopra indicati.

4.1.— In particolare, con riferimento all'art. 26, commi 1, secondo periodo, 2 e 3 della legge n. 289 del 2002, la Regione Emilia-Romagna, dopo avere ribadito il contenuto delle censure illustrate nel ricorso, sottolinea che la disposizione in esame non conterrebbe una «normativa tecnica», bensì una «disciplina amministrativa del Fondo», come sarebbe dimostrato dal contenuto del decreto ministeriale 14 ottobre 2003 (Disciplina delle procedure e modalità di funzionamento del Fondo per il finanziamento dei progetti di innovazione tecnologica nelle pubbliche amministrazioni e nel Paese, istituito dall'art. 26, comma 1, della legge 27 dicembre 2002, n. 289).

4.2.— In relazione all'art. 56 della stessa legge n. 289 del 2002, si contesta l'affermazione dell'Avvocatura generale dello Stato secondo cui la norma non violerebbe nessun principio costituzionale, attraverso il richiamo alle sentenze n. 49 e n. 16 del 2004, nonché n. 370 del 2003, che hanno dichiarato la illegittimità costituzionale di Fondi «destinati». Alla stessa conclusione – alla luce dei principî fissati nelle sentenze sopra indicate, nonché nella sentenza n. 14 del 2004 – si dovrebbe pervenire, secondo la ricorrente, anche nel caso in cui i Fondi siano direttamente erogati dallo Stato ai privati, dovendosi ritenere che gli stessi ledano «in misura ancora maggiore l'autonomia delle Regioni», le quali sarebbero del tutto escluse dalla gestione delle risorse in una materia di loro competenza.

4.3.— Quanto, infine, all'impugnazione dell'art. 27, comma 8, della legge n. 3 del 2003, la ricorrente, richiamando la sentenza n. 17 del 2004 della Corte, contesta la riconducibilità, addotta dall'Avvocatura generale dello Stato, dell'oggetto della disciplina della norma in esame alla materia del "coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale", a norma dell'art. 117, secondo comma, lettera *r*), della Costituzione. Si tratterebbe, infatti, di una disciplina «promozionale» dell'utilizzazione concreta degli strumenti informatici da parte delle amministrazione, nonché tipicamente organizzatoria, non affatto finalizzata «ad assicurare omogeneità di linguaggi informatici».

5.— L'Avvocatura generale dello Stato ha anch'essa depositato memorie in relazione ai ricorsi sopra indicati proposti dalla Regione Emilia-Romagna.

5.1.— In relazione all'art. 26, commi 1, secondo periodo, 2 e 3 della legge n. 289 del 2002, l'Avvocatura ha insistito per l'assunta infondatezza delle censure sulla base del rilievo che l'oggetto della disciplina, sia del primo che del secondo comma, dovrebbe essere ricondotto alla materia "coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale", di competenza legislativa esclusiva dello Stato, *ex* art. 117, secondo comma, lettera *r*), della Costituzione. In particolare, la difesa erariale sostiene che dette disposizioni «attengono unicamente al coordinamento sul piano tecnico delle varie iniziative di innovazione tecnologica, allo scopo di consentire, nella concorrente necessaria valutazione della economicità degli interventi, la comunione di linguaggio, di procedure e di *standard* omogenei in modo tale da permettere la più efficace comunicabilità tra i sistemi informatici delle varie amministrazioni».

In questa prospettiva, continua l'Avvocatura, il terzo comma dello stesso art. 26 – coinvolgendo in sede di Conferenza unificata sia le Regioni che gli enti locali «in tutti i provvedimenti», previsti sia dal primo che dal secondo comma della norma impugnata, qualora «riguardino l'organizzazione e la dotazione tecnologica» degli stessi enti – assicurerebbe una «adeguata ponderazione degli interessi e delle esigenze delle autonomie nell'esercizio dei poteri indubbiamente competenti allo Stato in materia allo stesso riservata».

5.2.— In relazione all'art. 56 della stessa legge n. 289 del 2002, la difesa erariale ha motivato la non fondatezza della questione sottolineando che – pur a volere ritenere che l'oggetto della disciplina della norma impugnata sia riconducibile alla materia concorrente della ricerca scientifica – non può attribuirsi al decreto del Presidente del Consiglio dei ministri, cui fa riferimento tale norma, natura regolamentare, con violazione dell'art. 117, sesto comma, della Costituzione. A detto decreto dovrebbe, infatti, riconoscersi

natura di provvedimento amministrativo, avendo lo stesso la sola funzione di riparto delle risorse «tra le diverse finalità» e di determinazione di «procedure, modalità e strumenti per l'utilizzo delle risorse» stesse.

La difesa erariale aggiunge, inoltre, che la norma impugnata – «nel quadro degli obiettivi di politica generale di sostegno e di coordinamento delle attività di ricerca scientifico-teconologica secondo le linee guida per la politica scientifica e tecnologica del Governo, approvate dal Cipe il 19 aprile 2002 e in coerenza con il VI Programma quadro di ricerca e sviluppo tecnologico dell'Unione europea 2002-2006» – sarebbe finalizzata alla «promozione di progetti strategici di ricerca scientifica e tecnologica che, per loro natura, hanno chiaramente una dimensione sovraregionale rapportandosi a temi prioritari per la salute, l'innovazione tecnologica, le grandi infrastrutture scientifiche», che richiedono e giustificano, in coerenza con i principî di adeguatezza e di sussidiarietà di cui all'art. 118 della Costituzione, la gestione unitaria a livello statale del relativo finanziamento.

5.3.— In relazione, infine, all'art. 27, comma 8, della legge n. 3 del 2003, la difesa erariale ha sottolineato che sarebbe possibile una interpretazione della norma conforme a Costituzione, ritenendo che la stessa si riferisca esclusivamente alle amministrazioni statali e agli enti pubblici nazionali. Questa interpretazione sarebbe confermata dal richiamo che la norma stessa fa al sesto comma dell'art. 117 della Costituzione, che conferisce potestà regolamentare allo Stato unicamente nelle materie di sua esclusiva competenza. Tale richiamo, continua la difesa erariale, «apparirebbe del tutto superfluo ove non fosse interpretato nel senso di ribadire (in modo sintetico e senza bisogno di ripetere nelle varie lettere della disposizione il medesimo concetto) i limiti al potere regolamentare dello Stato fissati nella norma stessa, che impediscono di incidere sull'organizzazione di Amministrazioni non statali».

Considerato in diritto

1.— Con ricorso (reg. ric. n. 25 del 2003) notificato il 1° marzo 2003 e depositato il successivo giorno 7, la Regione Emilia-Romagna ha impugnato numerose disposizioni della legge 27 dicembre 2002, n. 289 (Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato – legge finanziaria 2003), tra cui l'art. 26, commi 1, secondo periodo, 2 e 3, e l'art. 56, deducendo la violazione degli artt. 117, 118 e 119 della Costituzione, nonché del principio di leale collaborazione.

La stessa Regione Emilia-Romagna, con ricorso (reg. ric. n. 32 del 2003) notificato il 21 marzo 2003 e depositato il successivo giorno 27, ha impugnato diverse disposizioni della legge 16 gennaio 2003, n. 3 (Disposizioni ordinamentali in materia di pubblica amministrazione), tra cui l'art. 27, comma 8, deducendo la violazione dell'art. 117, quarto comma, della Costituzione.

Le impugnazioni delle citate disposizioni vengono trattate separatamente rispetto alle altre questioni proposte con gli stessi ricorsi e, per ragioni di omogeneità di materia, possono essere decise, previa riunione *in parte qua* dei giudizi, con la medesima sentenza.

2.— In particolare, con il ricorso n. 25 del 2003, la ricorrente ha impugnato l'art. 26, commi 1, secondo periodo, 2 e 3, della legge n. 289 del 2002, il quale prevede la istituzione di un «Fondo per il finanziamento di progetti di innovazione tecnologica nelle pubbliche amministrazioni e nel Paese», stabilendo che con decreti ministeriali «di natura non regolamentare» siano definite le modalità di funzionamento del Fondo stesso ed individuati «i progetti da finanziare e, ove necessario, la relativa ripartizione tra le amministrazioni interessate».

Secondo la Regione ricorrente tale disciplina, nella parte in cui si applica «alle Regioni, agli enti pararegionali e agli enti locali», si porrebbe in contrasto con l'art. 119 della Costituzione, in quanto, sancendo una «gestione ministeriale di un fondo speciale» in una materia di competenza legislativa residuale delle Regioni, quale quella relativa all'"organizzazione amministrativa regionale e degli enti locali", lederebbe l'autonomia finanziaria delle Regioni stesse. Risulterebbero, altresì, lese le potestà legislative e amministrative regionali, atteso che si conferiscono al Ministro, con norme dettagliate, «poteri sostanzialmente normativi ed amministrativi».

2.1.— Le censure formulate nei confronti dei commi 1, secondo periodo, e 2 dell'art. 26 non sono fondate nei termini di seguito precisati.

Il primo comma, primo periodo, con norma non oggetto di contestazione, istituisce un Fondo per il finanziamento di progetti di innovazione tecnologica nelle pubbliche amministrazioni e nel Paese. La seconda parte dello stesso primo comma, oggetto di specifica censura, prevede che il Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e il Ministro dell'economia

e delle finanze, con «uno o più decreti di natura non regolamentare», stabilisca le modalità di funzionamento del Fondo, individui i progetti da finanziare e, ove necessario, la relativa ripartizione, tra le amministrazioni interessate, delle risorse affluenti al Fondo stesso.

Il secondo comma dello stesso art. 26, invece – «al fine di assicurare una migliore efficacia della spesa informatica e telematica sostenuta dalle pubbliche amministrazioni, di generare significativi risparmi eliminando duplicazioni e inefficienze, promuovendo le migliori pratiche e favorendo il riuso, nonché di indirizzare gli investimenti nelle tecnologie informatiche e telematiche, secondo una coordinata e integrata strategia» – assegna al Ministro per l'innovazione e le tecnologie una serie di poteri riconducibili alle suddette finalità. In particolare il Ministro: a) definisce con proprie direttive le linee strategiche, la pianificazione e le aree di intervento dell'innovazione tecnologica nelle pubbliche amministrazioni, e ne verifica l'attuazione; b) approva, con il Ministro dell'economia e delle finanze, il piano triennale ed i relativi aggiornamenti annuali di cui all'art. 7 del decreto legislativo 12 febbraio 1993, n. 39, entro il 30 giugno di ogni anno; c) valuta la congruenza dei progetti di innovazione tecnologica che ritiene di grande valenza strategica rispetto alle direttive di cui alla lettera a) ed assicura il monitoraggio dell'esecuzione; d) individua i progetti intersettoriali che devono essere realizzati in collaborazione tra le varie amministrazioni interessate assicurandone il coordinamento e definendone le modalità di realizzazione; e) valuta, sulla base di criteri e metodiche di ottimizzazione della spesa, il corretto utilizzo delle risorse finanziarie per l'informatica e la telematica da parte delle singole amministrazioni; f) stabilisce le modalità con le quali le pubbliche amministrazioni comunicano le informazioni relative ai programmi informatici, realizzati su loro specifica richiesta, di cui esse dispongono, al fine di consentirne il riuso previsto dall'art. 25, comma 1, della legge 24 novembre 2000, n. 340; g) individua specifiche iniziative per i comuni con popolazione inferiore a 5.000 abitanti e per le isole minori; h) promuove l'informazione circa le iniziative per la diffusione delle nuove tecnologie.

2.2.— Le disposizioni di cui ai commi 1 e 2 dell'art. 26 si riferiscono, innanzitutto, all'amministrazione dello Stato e degli enti pubblici nazionali: per questa parte, pertanto, esse rinvengono la propria legittimazione nell'art. 117, secondo comma, lettere *g*) e *r*), della Costituzione, che assegnano alla competenza legislativa esclusiva statale, rispettivamente, le materie "ordinamento e organizzazione amministrativa dello Stato e degli enti pubblici nazionali" e "coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale".

2.3.— Le norme in questione sono suscettibili, però, di trovare applicazione anche nei confronti delle Regioni e degli enti locali, come risulta, tra l'altro, da quanto statuito nel terzo comma dello stesso art. 26, il quale prevede espressamente che i progetti – «di cui ai commi 1 e 2» – possono riguardare «l'organizzazione e la dotazione tecnologica delle Regioni e degli enti territoriali», e dispone che, in tal caso, è necessario sentire la Conferenza unificata di cui al decreto legislativo 28 agosto 1997, n. 281. Sotto tale aspetto, dunque, tali norme possono avere una diretta incidenza sulla «organizzazione amministrativa regionale e degli enti locali», ma ciò non determina alcuna violazione – nei limiti in cui siano garantite adeguate procedure collaborative – delle competenze della ricorrente. Le disposizioni in esame, infatti, devono essere interpretate, conformemente a Costituzione, nel senso che le stesse – nella parte in cui riguardano Regioni ed enti territoriali – costituiscono espressione della potestà legislativa esclusiva statale nella materia del "coordinamento informativo statistico e informatico dei dati dell'amministrazione statale, regionale e locale", *ex* art. 117, secondo comma, lettera *r*), della Costituzione.

Questa Corte ha, in proposito, già avuto modo di sottolineare che l'attribuzione a livello centrale della suddetta materia si giustifica alla luce della necessità di «assicurare una comunanza di linguaggi, di procedure e di *standard* omogenei, in modo da permettere la comunicabilità tra i sistemi informatici della pubblica amministrazione» (sentenza n. 17 del 2004).

2.4.— Ne consegue, pertanto, che «i progetti da finanziare» cui fa riferimento il primo comma dell'art. 26 della legge n. 289 del 2002 – nella misura in cui «riguardino l'organizzazione e la dotazione tecnologica delle Regioni e degli enti territoriali» (comma 3) – possono essere esclusivamente quelli aventi una connotazione riconducibile a siffatta finalità di coordinamento tecnico. Del resto, lo stesso decreto ministeriale 14 ottobre 2003 di attuazione della disposizione in esame ha indicato, tra i «progetti finanziabili», anche quelli idonei a promuovere «l'interoperabilità e la cooperazione applicativa tra pubbliche amministrazioni» (art. 2, comma 1).

2.5.— Allo stesso modo la norma contenuta nell'art. 26, comma 2, deve essere intesa – nella parte in cui riguarda Regioni ed enti locali – come attributiva al Ministro della innovazione e delle tecnologie di un

potere limitato ad un coordinamento meramente tecnico. Questa interpretazione è suffragata dalle medesime finalità indicate nella disposizione in esame: «assicurare una migliore efficacia della spesa informatica e telematica»; «generare significativi risparmi eliminando duplicazioni e inefficienze, promuovendo le migliori pratiche e favorendo il riuso»; «indirizzare gli investimenti nelle tecnologie informatiche e telematiche, secondo una coordinata e integrata strategia». Sul punto, questa Corte, nella sentenza n. 17 del 2004, ha, infatti, precisato che «attengono al predetto coordinamento anche i profili della qualità dei servizi e della razionalizzazione della spesa in materia informatica», ove ritenuti necessari al fine di garantire la omogeneità nella elaborazione e trasmissione dei dati.

2.6.— La questione relativa al comma 3 dello stesso art. 26 è, invece, fondata.

La norma in esame dispone che deve essere sentita la Conferenza unificata nei casi in cui i progetti di cui ai commi 1 e 2 «riguardino l'organizzazione e la dotazione tecnologica delle Regioni e degli enti territoriali».

La previsione del mero parere della Conferenza unificata non costituisce, nella specie, una misura adeguata a garantire il rispetto del principio di leale collaborazione. Per quanto l'oggetto delle norme di cui ai commi 1 e 2, cui rinvia la disposizione in esame, sia riconducibile, nei limiti esposti, alla materia del "coordinamento informativo statistico e informatico" di spettanza esclusiva del legislatore statale, lo stesso presenta un contenuto precettivo idoneo a determinare una forte incidenza sull'esercizio concreto delle funzioni nella materia dell'"organizzazione amministrativa delle Regioni e degli enti locali". Ciò rende necessario garantire un più incisivo coinvolgimento di tali enti nella fase di attuazione delle disposizioni censurate mediante lo strumento dell'intesa: da qui la illegittimità costituzionale dell'art. 26, comma 3, della legge n. 289 del 2002 nella parte in cui prevede che sia «sentita la Conferenza unificata» anziché che si raggiunga con la stessa Conferenza l'intesa.

3.— Con lo stesso ricorso (reg. ric. n. 25 del 2003) la Regione Emilia-Romagna ha, altresì, impugnato l'art. 56 della legge n. 289 del 2002, che ha «istituito un Fondo finalizzato al finanziamento di progetti di ricerca, di rilevante valore scientifico, anche con riguardo alla tutela della salute e all'innovazione tecnologica, con una dotazione finanziaria di 225 milioni di euro per l'anno 2003 e di 100 milioni di euro a decorrere dall'anno 2004». Lo stesso articolo stabilisce, inoltre, che: alla «ripartizione del Fondo, istituito nello stato di previsione del Ministero dell'economia e delle finanze, tra le diverse finalità provvede il Presidente del Consiglio dei Ministri, con proprio decreto, su proposta del Ministro dell'istruzione, dell'università e della ricerca, sentiti i Ministri dell'economia e delle finanze, della salute e per l'innovazione tecnologica. Con lo stesso decreto sono stabiliti procedure, modalità e strumenti per l'utilizzo delle risorse, assicurando in via prioritaria il finanziamento dei progetti presentati da soggetti che abbiano ottenuto, negli anni precedenti, un eccellente risultato nell'utilizzo e nella capacità di spesa delle risorse comunitarie assegnate e delle risorse finanziarie provenienti dai programmi quadro di ricerca dell'Unione europea o dai Fondi strutturali».

Secondo la ricorrente tale disposizione – istituendo un «Fondo settoriale a gestione centrale» e attribuendo con norme di dettaglio «poteri sostanzialmente normativi ed amministrativi al Presidente del Consiglio dei Ministri» – violerebbe gli artt. 117, terzo e sesto comma, 118, secondo comma, e 119 della Costituzione.

La questione non è fondata nei termini di seguito precisati.

La ricerca scientifica e tecnologica nel nuovo testo dell'art. 117 della Costituzione è inclusa tra le materie appartenenti alla competenza concorrente.

Tuttavia, questa Corte, con sentenza n. 423 del 2004, ha affermato cheSulla base di tali premesse la Corte ha ritenuto, innanzitutto, ammissibile un intervento "autonomo" statale in relazione alla disciplina delle «istituzioni di alta cultura, università ed accademie», che «hanno il diritto di darsi ordinamenti autonomi nei limiti stabiliti dalle leggi dello Stato» (art. 33, sesto comma, Cost.). Detta norma ha, infatti, previsto una "riserva di legge" statale (sentenza n. 383 del 1998), che ricomprende in sé anche quei profili relativi all'attività di ricerca scientifica che si svolge, in particolare, presso le strutture universitarie (art. 63 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, recante "Riordinamento della docenza universitaria, relativa fascia di formazione nonché sperimentazione organizzativa e didattica").

Al di fuori di questo ambito lo Stato conserva, inoltre, una propria competenza in relazione ad attività di ricerca scientifica strumentale e intimamente connessa a funzioni statali, allo scopo di assicurarne un migliore espletamento, sia organizzando direttamente le attività di ricerca, sia promuovendo studi finalizzati (cfr. sentenza n. 569 del 2000).

Infine, il legislatore statale – come questa Corte ha precisato con la citata sentenza n. 423 del 2004 – può sempre, nei casi in cui sussista «la potestà legislativa concorrente nella "materia" in esame, non solo ovviamente fissare i principî fondamentali, ma anche attribuire con legge funzioni amministrative a livello centrale, per esigenze di carattere unitario, e regolarne al tempo stesso l'esercizio – nel rispetto dei principî di sussidiarietà, differenziazione ed adeguatezza – mediante una disciplina che sia logicamente pertinente e che risulti limitata a quanto strettamente indispensabile a tali fini» (vedi anche sentenze n. 6 del 2004 e n. 303 del 2003).

Alla luce delle osservazioni che precedono, la disposizione censurata deve essere interpretata nel senso che la stessa è finalizzata a finanziare esclusivamente quei progetti di ricerca in relazione ai quali è configurabile, nei limiti indicati, un autonomo titolo di legittimazione del legislatore statale. Da ciò consegue che tale disposizione, così interpretata, non determina alcun *vulnus* a competenze regionali.

4.— Con altro ricorso (reg. ric. n. 32 del 2003) notificato il 21 marzo 2003 e depositato il successivo giorno 27, la stessa Regione Emilia-Romagna ha impugnato l'art. 27, comma 8, della legge 16 gennaio 2003, n. 3, per violazione dell'art. 117, quarto comma, della Costituzione.

Tale norma prevede che, entro un anno dalla data di entrata in vigore della suddetta legge, siano «emanati uno o più regolamenti, ai sensi dell'articolo 117, sesto comma, della Costituzione e dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, per introdurre nella disciplina vigente le norme necessarie ai fini del conseguimento dei seguenti obiettivi: a) diffusione dei servizi erogati in via telematica ai cittadini e alle imprese, anche con l'intervento dei privati, nel rispetto dei principî di cui all'articolo 97 della Costituzione e dei provvedimenti già adottati; b) diffusione e uso della carta nazionale dei servizi; c) diffusione dell'uso delle firme elettroniche; d) ricorso a procedure telematiche da parte della pubblica amministrazione per l'approvvigionamento di beni e servizi, potenziando i servizi forniti dal Ministero dell'economia e delle finanze attraverso la CONSIP Spa (Concessionaria servizi informativi pubblici); e) estensione dell'uso della posta elettronica nell'ambito delle pubbliche amministrazioni e dei rapporti tra pubbliche amministrazioni e privati; f) generalizzazione del ricorso a procedure telematiche nella contabilità e nella tesoreria; g) alfabetizzazione informatica dei pubblici dipendenti; h) impiego della telematica nelle attività di formazione dei dipendenti pubblici; i) diritto di accesso e di reclamo esperibile in via telematica da parte dell'interessato nei confronti delle pubbliche amministrazioni».

Secondo la ricorrente, la norma riportata inciderebbe «essenzialmente sulla materia dell'organizzazione interna delle Regioni, degli enti locali e degli enti pubblici di carattere regionale», nonché sulla materia della formazione professionale, [lettere *g*) e *h*) della disposizione impugnata]. In presenza, pertanto, di materie di competenza regionale sarebbe illegittima la previsione di un regolamento statale *ex* art. 117, sesto comma, della Costituzione, che «potrà valere per lo Stato e per gli enti pubblici nazionali, mentre spetta alle Regioni la disciplina per le amministrazioni cui si riferisce la legislazione regionale».

4.1.— La questione non è fondata nei termini di seguito precisati.

Il comma 8 dell'art. 27 della legge n. 3 del 2003 indica taluni "obiettivi" da perseguire per la realizzazione di un vasto processo di "innovazione tecnologica nella pubblica amministrazione". Si tratta di obiettivi genericamente posti, che dovranno essere attuati mediante l'emanazione di uno o più regolamenti ai sensi dell'art. 17, comma 2, della legge n. 400 del 1988 e che coincidono sostanzialmente con gli "obiettivi di legislatura" contenuti nelle «Linee guida del Governo per lo sviluppo della Società dell'Informazione nella legislatura», emanate dal Consiglio dei ministri in data 31 maggio 2002.

Della disposizione impugnata è possibile dare una interpretazione conforme alle previsioni contenute nel nuovo Titolo V, Parte II, della Costituzione, potendosi ritenere che le procedure e i servizi telematici dalla stessa disposizione disciplinati abbiano quali unici destinatari le amministrazioni dello Stato e gli enti pubblici nazionali. Ne consegue che i generici riferimenti alla locuzione "pubblica amministrazione" contenuti nella norma censurata devono intendersi riferiti esclusivamente all'amministrazione statale nel senso sopra precisato, con esclusione degli enti regionali. Tale interpretazione risulta conforme a Costituzione, in quanto l'art. 117, secondo comma, lettera *g*), Cost., attribuisce in via esclusiva alla competenza legislativa statale la materia dell'"organizzazione amministrativa dello Stato e degli enti pubblici nazionali".

Sotto altro aspetto non può ritenersi, come affermato dalla ricorrente, che le previsioni di cui alla lettera *g*) – «alfabetizzazione informatica dei pubblici dipendenti» – ed alla lettera *h*) – «impiego della telematica nelle attività di formazione dei dipendenti pubblici» – dello stesso art. 27, comma 8, della legge in esame, debbano essere ricondotte alla materia della "formazione professionale" di competenza legislativa

residuale delle Regioni. Ciò in quanto l'acquisizione delle competenze necessarie per l'utilizzo delle tecnologie dell'informazione da parte dei "pubblici dipendenti" (da intendersi statali) persegue pur sempre finalità connesse alla innovazione tecnologica nell'ambito dell'organizzazione amministrativa dello Stato e, dunque, è riconducibile alla potestà legislativa esclusiva dello Stato stesso.

La prospettata interpretazione è, del resto, confermata dalla stessa disposizione impugnata che, demandando a uno o più regolamenti di introdurre nella disciplina vigente le norme necessarie ai fini del conseguimento degli obiettivi indicati, fa espresso richiamo al sesto comma dell'art. 117 della Costituzione, che attribuisce allo Stato la potestà regolamentare soltanto nelle materie rientranti nell'ambito della propria competenza legislativa esclusiva.

PER QUESTI MOTIVI
LA CORTE COSTITUZIONALE

riservata a separate pronunce la decisione delle altre questioni sollevate con i ricorsi n. 25 e n. 32 del registro ricorsi 2003;

riuniti i giudizi;

a) *dichiara* l'illegittimità costituzionale dell'art. 26, comma 3, della legge 27 dicembre 2002, n. 289 (Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato – legge finanziaria 2003), nella parte in cui prevede che qualora i progetti cui si riferiscono i commi 1 e 2 dello stesso art. 26 riguardino l'organizzazione e la dotazione tecnologica delle Regioni e degli enti territoriali «i provvedimenti sono adottati sentita la Conferenza unificata di cui all'art. 8 del decreto legislativo 28 agosto 1997, n. 281», anziché stabilire che tali provvedimenti sono adottati previa intesa con la Conferenza stessa;

b) *dichiara* non fondata, nei sensi di cui in motivazione, la questione di legittimità costituzionale dell'art. 26, commi 1 e 2, della predetta legge n. 289 del 2002, sollevata dalla Regione Emilia-Romagna, in riferimento agli artt. 117, 118 e 119 della Costituzione, con il ricorso indicato in epigrafe;

c) *dichiara* non fondata, nei sensi di cui in motivazione, la questione di legittimità costituzionale dell'art. 56 della predetta legge n. 289 del 2002, sollevata dalla Regione Emilia-Romagna, in riferimento agli artt. 117, 118 e 119 della Costituzione, con il ricorso indicato in epigrafe;

d) *dichiara* non fondata, nei sensi di cui in motivazione, la questione di legittimità costituzionale dell'art. 27, comma 8, della legge 16 gennaio 2003, n. 3 (Disposizioni ordinamentali in materia di pubblica amministrazione), sollevata dalla Regione Emilia-Romagna, in riferimento all'art. 117 della Costituzione, con il ricorso indicato in epigrafe.

Così deciso in Roma, nella sede della Corte costituzionale, Palazzo della Consulta, il 12 gennaio 2005.

Si segnala la sezione dedicata all' "Informatica pubblica" nel sito del Consiglio di Stato e dei Tribunali Amministrativi Regionali.

NUMERO SCHEDA: 6131

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: GIUSTIZIA AMMINISTRATIVA

Sul sito del Consiglio di Stato e dei Tribunali Amministrativi Regionali (http://www.giustizia-amministrativa.it) c'è una sezione nella quale vengono raccolti articoli (al momento si tratta di commenti di magistrati, professori universitari ed avvocati) concernenti un settore sempre più attuale della pubblica amministrazione, quello dell' "Informatica pubblica".

Per accedere alla sezione in oggetto bisogna cliccare sull'icona "Studi e Contributi", poi su "indice per materia", quindi su "Pubblica amministrazione", sezione "Informatica pubblica".
Il link diretto alla sezione dedicata alla dottrina è: http://www.giustizia-amministrativa.it/webcds/dottrina.htm#18

Attualmente sono disponibili i seguenti commenti.

PUBBLICA AMMINISTRAZIONE - *Informatica pubblica*

Cardarelli, F., (professore associato di istituzioni di diritto pubblico), *Le banche dati pubbliche: una definizione;*

Giurdanella, C.,(Avvocato del Foro di Catania), *Depositi "elettronici" al Tar Catania: spunti per un processo amministrativo telematico; (dicembre 2004)*

Liccardo, P., (Magistrato del Tribunale di Bologna), *Introduzione al processo civile telematico;*

Sorrentino. F. (Magistrato di Cassazione), *E' arrivato il "codice della privacy"* (con molti dubbi di costituzionalità)*. Limiti e problemi nel controllo sull'autorità giudiziaria;* (marzo 2004)

Sorrentino, F. (Magistrato di Cassazione), Firma digitale e firma elettronica: stato attuale e prospettive di riforma;

Sorrentino, F. (Magistrato di Cassazione), Il c.d. processo telematico;

Sorrentino. F. (Magistrato di Cassazione), *Nuova disciplina sulle firme elettroniche: luci ed ombre dell'intervento normativo;*

Sorrentino. F. (Magistrato di Cassazione), *La disciplina sulle firme elettroniche: ultimo tassello?* (marzo 2004);

Torsello, M. (Consigliere di Stato)- Minerva, M. , (Consigliere Corte dei conti) Documento informatico e pubblica amministrazione- Commento agli articoli 18-22 del d.P.R. 10 novembre 1997, n. 513 - Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici;

Un interessante articolo su "Dodici anni di legimatica. Da una parola a una disciplina".

NUMERO SCHEDA: 6112

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: ITER LEGIS: INFORMAZIONE E CRITICA LEGISLATIVA

AUTORE: Pietro Mercatali

NUMERO: 1

DATA: 28/02/2005

PAGINA: 97-118

NATURA ATTO: COMMENTO

Sulla rivista "Iter legis" (n. 6/2004-1/2005) è pubblicato questo interessante articolo dal titolo "Dodici anni di legimatica. Da una parola ad una disciplina", a cura di Pietro Mercatali, in visione presso il settore Studi e documentazione legislativi.
Il commento, ricchissimo di note e riferimenti bibilografici, partendo dalla definizione del vocabolo legimatica affronta il percorso e l'evoluzione di questo particolare settore dell'informatica giuridica nonché la sua utilizzazione sia in ambiti istituzionali che non istituzionali, sia in Italia che in altri stati.
Il commento si suddivide nei seguenti capitoli:
- 1. "Premessa metodologica: la parola legimatica nel web".
- 2. "Legimatica: prime attestazioni e definizioni".
- 3. "Progetti di ricerca tra teoria e applicazione".
- 4. "La legimatica nelle istituzioni legislative, nelle professioni e nelle imprese".
- 5. "La legimatica nel mondo accademico e nell'insegnamento universitario".
- 6. "La legimatica sui mezzi di comunicazione di massa".

Pubblicato sulla Gazzetta Ufficiale il regolamento di attuazione della legge stanca che rende piu' accessibili i servizi web della p.a.

NUMERO SCHEDA: 6003

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: GAZZETTA UFFICIALE

NUMERO: 101

DATA: 03/05/2005

RIFERIMENTO NORMATIVO: legge n. 4/2004

NATURA ATTO: DECRETO PRESIDENTE DELLA REPUBBLICA

DATA ATTO: 01/03/2005

NUM. ATTO: 75

Il Regolamento di attuazione della legge n. 4 del 9 gennaio 2004 (c.d. Legge Stanca) recante disposizioni per favorire l'accesso dei disabili agli strumenti informatici, approvato in via definitiva dal Consiglio dei ministri in data 25 febbraio 2005, è stato pubblicato sulla Gazzetta Ufficiale n. 101 del 3 maggio 2005.
Il regolamento, approvato con D.P.R. 1 marzo 2005, n. 75, prevede che entro 12 mesi dalla sua pubblicazione tutti gli uffici pubblici debbano adeguare i loro servizi sul web alle nuove regole sull'accessibilità, pena la nullità dei contratti di gestione.
Il regolamento, finalizzato ad evitare forme di emarginazione causate dalle nuove tecnologie ed a promuovere l'uso di queste anche quale strumento di miglioramento della qualità della vita, è stato redatto con il contributo delle più rappresentative Associazioni che operano nel settore della disabilità, nonché di competenti operatori in materia di accessibilità di tecnologie informatiche.
Per ottenere il "bollino" che certifica l'accessibilità al sito internet, gli uffici pubblici dovranno autocertificare il rispetto delle regole tecniche indicate da un prossimo decreto ministeriale che sarà pubblicato in G.U. contestualmente al regolamento sull'accessibilità.
Il regolamento, inoltre, impone che in ciascuna p.a. centrale sia nominato tra i dirigenti un responsabile all'accessibilità informatica, altrimenti si considera designato al ruolo il responsabile dei sistemi informatici.
Spetta al Centro nazionale per informatica nella pubblica amministrazione (Cnipa) il compito di monitorare il rispetto dei requisiti per l'accessibilità e in caso di accertamento negativo sono annullati tutti i contratti di gestione del sito web. Le regioni, gli enti locali e le province autonome, invece, dovranno organizzarsi autonomamente per vigilare sull'attuazione delle nuove norme.
Anche i privati possono ricorrere alla certificazione ma l'ipotesi è assolutamente facoltativa.

Si riporta il testo del regolamento.

Si segnala un commento al d.p.r. sulla rivista "Guida agli enti locali", n. 23/2005, pp. 42 e 45, a cura di Paolo Subioli, consultabile presso il settore Studi e documentazione legislativi.

Si riporta anche l'art. 53 del d.lgs. n. 82/2005 "Codice dell'amministrazione digitale", che prevede che i siti istituzionali delle pubbliche amministrazioni rispettino, fra gli altri, il principio di accessibilità.

D.P.R. 1 marzo 2005, n. 75 (1).

Regolamento di attuazione della L. 9 gennaio 2004, n. 4, per favorire l'accesso dei soggetti disabili agli strumenti informatici.

(1) Pubblicato nella Gazz. Uff. 3 maggio 2005, n. 101.

1. Definizioni.
1. Ai fini del presente regolamento s'intende per:
a) accessibilità: ai sensi dell'articolo 2, comma 1, lettera a), della legge 9 gennaio 2004, n. 4, la capacità dei sistemi informatici, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari;
b) tecnologie assistive: ai sensi dell'articolo 2, comma 1, lettera b), della legge n. 4 del 2004, gli strumenti e le soluzioni tecniche, hardware e software, che permettono alla persona disabile, superando o riducendo le condizioni di svantaggio, di accedere ai servizi erogati dai sistemi informatici;
c) valutazione: processo con il quale si riscontra la rispondenza dei servizi ai requisiti di accessibilità;
d) verifica tecnica: valutazione condotta da esperti, anche con strumenti informatici, sulla base di parametri tecnici;
e) verifica soggettiva: valutazione del livello di qualità dei servizi, già giudicati accessibili tramite la verifica tecnica, effettuata con l'intervento del destinatario, anche disabile, sulla base di considerazioni empiriche;
f) fruibilità: la caratteristica dei servizi di rispondere a criteri di facilità e semplicità d'uso, di efficienza, di rispondenza alle esigenze dell'utente, di gradevolezza e di soddisfazione nell'uso del prodotto;
g) soggetti privati: soggetti diversi da quelli di cui all'articolo 3 della legge n. 4 del 2004;
h) valutatori: soggetti iscritti nell'apposito elenco e qualificati a certificare le caratteristiche di accessibilità dei servizi.
2. Criteri e princìpi generali per l'accessibilità.
1. Sono accessibili i servizi realizzati tramite sistemi informatici che presentano i seguenti requisiti:
a) accessibilità al contenuto del servizio da parte dell'utente;
b) fruibilità delle informazioni offerte, caratterizzata anche da:
1) facilità e semplicità d'uso, assicurando, fra l'altro, che le azioni da compiere per ottenere servizi e informazioni siano sempre uniformi tra loro;
2) efficienza nell'uso, assicurando, fra l'altro, la separazione tra contenuto, presentazione e modalità di funzionamento delle interfacce, nonché la possibilità di rendere disponibile l'informazione attraverso differenti canali sensoriali;
3) efficacia nell'uso e rispondenza alle esigenze dell'utente, assicurando, fra l'altro, che le azioni da compiere per ottenere in modo corretto servizi e informazioni siano indipendenti dal dispositivo utilizzato per l'accesso;
4) soddisfazione nell'uso, assicurando, fra l'altro, l'accesso al servizio e all'informazione senza ingiustificati disagi o vincoli per l'utente;
c) compatibilità con le linee guida indicate nelle comunicazioni, nelle raccomandazioni e nelle direttive sull'accessibilità dell'Unione europea, nonché nelle normative internazionalmente riconosciute e tenendo conto degli indirizzi forniti dagli organismi pubblici e privati, anche internazionali, operanti nel settore, quali l'International Organization for Standardization (ISO) e il World Wide Web Consortium (W3C).
2. Con apposito decreto del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro dell'istruzione, dell'università e della ricerca, sentiti la Conferenza unificata e il Centro nazionale per l'informatica nella pubblica amministrazione (Cnipa), sono dettate specifiche regole tecniche che disciplinano 1'accessibilità, da parte degli utenti, agli strumenti didattici e formativi di cui all'articolo 5, comma 1, della legge n. 4 del 2004.
3. Valutazione dell'accessibilità.
1. Il Cnipa, con proprio provvedimento, istituisce presso di sé l'elenco dei valutatori, stabilendone le modalità tecniche per la tenuta, nonché garantisce la pubblicità dell'elenco medesimo e delle citate modalità sul proprio sito internet.
2. Nell'elenco di cui al comma 1 sono iscritte le persone giuridiche interessate che ne fanno richiesta, dimostrando di possedere i seguenti requisiti:
a) garanzia di imparzialità ed indipendenza nell'esercizio delle proprie attività;
b) disponibilità di una adeguata strumentazione per l'applicazione delle metodologie di verifica tecnica e di verifica soggettiva di cui all'articolo 1, comma 1, rispettivamente, lettere d) ed e);
c) disponibilità di figure professionali esperte nelle suddette metodologie di verifica e di figure idonee ad interagire con i soggetti con specifiche disabilità.

3. Ai fini dei requisiti di cui al comma 2, lettera a), il valutatore, all'atto della richiesta di iscrizione, si impegna:
a) a non esprimere valutazioni su siti o servizi dallo stesso realizzati;
b) a non esprimere valutazioni in tutti i casi in cui queste possano avere un'incidenza specifica su interessi propri del valutatore o di soggetti allo stesso collegati da rapporti societari;
c) una volta effettuata la valutazione, a non fornire, nell'arco dei ventiquattro mesi successivi, attività di implementazione sui siti o servizi per i quali sia stato incaricato di esprimere la valutazione stessa.
4. Nell'accertamento dei requisiti di accessibilità dei servizi, acquisiti con le procedure o realizzati tramite i contratti di cui all'articolo 4, commi 1 e 2, della legge n. 4 del 2004, le amministrazioni interessate possono acquisire il parere non vincolante di un valutatore iscritto nell'elenco di cui al comma 1.
5. Con il decreto del Ministro per l'innovazione e le tecnologie, di cui all'articolo 11 della legge n. 4 del 2004, sono stabiliti:
a) le specifiche tecniche per la sussistenza dei requisiti di cui al comma 2, lettere b) e c);
b) gli importi massimi dovuti dai soggetti privati come corrispettivo per l'attività svolta dai valutatori di cui al comma 1, tenuto conto dei costi di organizzazione aziendale nella misura minima, maggiorati del dieci per cento;
c) le somme dovute dai soggetti privati quale rimborso delle spese amministrative sostenute dalla Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie per l'attività di cui all'articolo 4, comma 1, nonché l'entità della quota dovuta al Cnipa nei casi previsti dall'articolo 7, comma 2, per l'espletamento delle funzioni ispettive di cui al medesimo articolo 7.
6. Il venire meno dei requisiti in base ai quali è avvenuta l'iscrizione determina la cancellazione dall'elenco di cui al comma 1; la cancellazione è altresì disposta nel caso di violazione degli obblighi assunti dal valutatore ai sensi del comma 3.
7. Nei casi di cui al comma 6, il Cnipa comunica al valutatore che intende procedere, trascorsi trenta giorni, alla cancellazione dello stesso dall'elenco; l'interessato può presentare proprie memorie al riguardo. Il Cnipa provvede altresì a dare adeguata pubblicità della avvenuta cancellazione sul proprio sito internet.
4. Modalità di richiesta della valutazione.
1. I soggetti privati richiedono alla Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie l'autorizzazione ad utilizzare il logo, allegando l'attestato di cui al comma 2. L'utilizzazione del logo è limitata al periodo di validità dell'attestato.
2. I soggetti privati si rivolgono ad uno dei valutatori che, svolta la sua attività, in caso di esito positivo, rilascia attestato di accessibilità, con validità non superiore a dodici mesi, eventualmente indicante il livello di qualità raggiunto di cui all'articolo 5.
3. La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, ai fini dell'adozione del provvedimento di cui al comma 1 si avvale, tramite apposita convenzione, del Cnipa.
4. All'attuazione del presente articolo si provvede nell'àmbito degli ordinari stanziamenti di bilancio, senza nuovi o maggiori oneri per la finanza pubblica.
5. Logo attestante il possesso del requisito di accessibilità.
1. Il logo che attesta il superamento della sola verifica tecnica raffigura un personal computer di colore terra di Siena, unito a tre figure umane stilizzate rispettivamente, da sinistra, di colore celeste, azzurro e amaranto, le quali fuoriescono dallo schermo a braccia levate; all'esito della verifica soggettiva, il diverso livello di qualità raggiunto dal servizio è indicato mediante asterischi, da uno a tre, riportati nella parte del logo raffigurante la tastiera del personal computer.
2. La corrispondenza tra il logo, eventualmente corredato da asterischi, ed il diverso livello di qualità dei servizi, nonché il modello del logo stesso sono indicati nel decreto di cui all'articolo 11 della legge n. 4 del 2004.
6. Casi di aggiornamento della valutazione di accessibilità.
1. In caso di modifiche sostanziali dei siti o servizi e nel caso del rinnovo dell'autorizzazione di cui all'articolo 4, comma 1, i soggetti privati richiedono tempestivamente un aggiornamento della valutazione dell'accessibilità ad uno dei valutatori iscritti nell'elenco. Il valutatore, effettuata la verifica, rilascia un nuovo attestato al soggetto richiedente, inviandone contestualmente copia all'amministrazione per l'aggiornamento della durata e del livello di qualità del logo; in caso di rinnovo dell'autorizzazione l'invio della copia deve avvenire almeno quindici giorni prima della data di scadenza dell'autorizzazione stessa.
7. Poteri ispettivi di controllo sui soggetti privati.

1. Nei riguardi dei soggetti privati, il Cnipa, previa comunicazione inviata al soggetto interessato, verifica il mantenimento dei requisiti di accessibilità dei siti e dei servizi, anche avvalendosi di valutatori iscritti nell'elenco di cui all'articolo 3, comma 1, purché questi ultimi risultino estranei alla realizzazione, manutenzione o certificazione del sito o servizio, e adegua eventualmente il logo al livello di accessibilità riscontrata aggiornandone la validità temporale.
2. In caso di riscontro di un livello di accessibilità inferiore a quello del logo utilizzato sono a carico del soggetto privato i costi effettivi dell'avvenuta ispezione, nonché una quota di partecipazione ai costi per l'espletamento delle funzioni ispettive determinata ai sensi dell'articolo 3, comma 5, lettera c), e comunque di importo non superiore al doppio del costo effettivo dell'ispezione.
8. Modalità di utilizzo del logo da parte dei soggetti di cui al comma 1, dell'articolo 3 della legge n. 4 del 2004.
1. Le amministrazioni pubbliche e comunque i soggetti di cui all'articolo 3, comma 1, della legge n. 4 del 2004, che intendono utilizzare il logo sui siti e sui servizi forniti, provvedono autonomamente a valutare l'accessibilità sulla base delle regole tecniche definite con il decreto del Ministro per l'innovazione e le tecnologie, di cui all'articolo 11 della legge n. 4 del 2004; la valutazione positiva, previa segnalazione al Cnipa, consente l'utilizzo del logo.
9. Controlli esercitabili sui soggetti di cui al comma 1, dell'articolo 3 della legge n. 4 del 2004.
1. Per l'attuazione della legge ogni amministrazione pubblica centrale nomina un responsabile dell'accessibilità informatica, da individuare tra il personale appartenente alla qualifica dirigenziale già in servizio presso l'amministrazione stessa, la cui funzione, in assenza di specifica designazione, è svolta dal responsabile dei sistemi informativi, di cui all'articolo 10 del decreto legislativo n. 39 del 1993; dall'attuazione del presente comma non derivano nuovi o maggiori oneri a carico delle amministrazioni interessate e per lo svolgimento di tale funzione non è previsto compenso aggiuntivo.
2. Ai sensi dell'articolo 7, comma 1, lettera b), della legge n. 4 del 2004, la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, avvalendosi del Cnipa, previa comunicazione inviata all'amministrazione statale interessata, verifica il mantenimento dei requisiti di accessibilità dei siti e dei servizi forniti e dà notizia dell'esito di tale verifica al dirigente responsabile; qualora siano riscontrate anomalie, viene richiesta all'amministrazione statale medesima la predisposizione del relativo piano di adeguamento con l'indicazione delle attività e dei tempi di realizzazione.
3. Le regioni, le province autonome e gli enti locali organizzano autonomamente e secondo i propri ordinamenti la vigilanza sull'attuazione del presente regolamento.
4. Il Ministro per l'innovazione e le tecnologie, sulla base degli esiti delle verifiche di cui al comma 2, riferisce annualmente al Parlamento, dandone altresì comunicazione alla Conferenza unificata.
Art. 53 del d.lgs. n. 82/2005 “Codice dell’amministrazione digitale”.
Art. 53. Caratteristiche dei siti.
1. Le pubbliche amministrazioni centrali realizzano siti istituzionali su reti telematiche che rispettano i princìpi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità dì consultazione, qualità, omogeneità ed interoperabilità.
2. Il CNIPA svolge funzioni consultive e di coordinamento sulla realizzazione e modificazione dei siti delle amministrazioni centrali.
3. Lo Stato promuove intese ed azioni comuni con le regioni e le autonomie locali affinché realizzino siti istituzionali con le caratteristiche di cui al comma 1.

Un interessante articolo sul documento informatico.

NUMERO SCHEDA: 5756

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: RIVISTA DI DIRITTO CIVILE

AUTORE: A. Masucci

NUMERO: 5

DATA: 31/10/2004

PAGINA: 749-786

NATURA ATTO: COMMENTO

Si tratta di un articolo interessante e particolareggiato a cura di Alfonso Masucci, intitolato "*Il documento informatico. profili ricostruttivi della nozione e della disciplina*".
Il commento, particolarmente ricco di riferimenti dottrinali e legislativi, affronta, in 19 capitoli, tutti gli aspetti, più o meno controversi, di questo particolare tipo di documento.
Per quanto concerne la parte relativa alle problematiche della sottoscrizione elettronica si segnala il capitolo 14, intitolato "*La particolare disciplina prevista per la sottoscrizione dei documenti delle pubbliche amministrazioni. L'obbligo della firma digitale e i limiti a questo obbligo*".

Il commento è consultabile presso il settore Studi e documentazione legislativi.

Una direttiva del ministero dell'innovazione contiene le linee guida per la seconda fase della digitalizzazione della p.a.

NUMERO SCHEDA: 5755

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: ITALIA OGGI

DATA: 11/01/2005

NATURA ATTO: DIRETTIVA

Il Ministro dell'Innovazione ha emanato una direttiva contenente le linee guida relative alla c.d. seconda fase della digitalizzazione della p.a. Tale seconda fase parte dopo la conclusione di un primo momento i cui risultati sono stati messi in luce in una nota del Ministro stesso. In particolare, si evidenzia, negli ultimi anni, si è avuta una diffusione nell'uso della posta elettronica tra i dipendenti pubblici, sono state distribuite oltre 600 mila firme digitali, 23 mila delle quali ai funzionari statali che le usano per siglare circa 3 mila mandati di pagamento al giorno e sono stati 25 milioni gli impegni di spesa pubblica emessi on-line.
I punti principali della citata direttiva sono così riassumibili:

- invito rivolto agli uffici pubblici a sviluppare l'uso degli strumenti telematici per ridurre gli oneri di archiviazione e di spedizione dei documenti;
- sollecitazione agli enti statali circa la promozione dell'interattività nell'erogazione dei servizi ai cittadini;
- maggiore utilizzo della telefonata via internet attraverso la tecnologia denominata "voice over ip" che consente il trasferimento delle comunicazioni attraverso i normali server piuttosto che con le attuali centrali telefoniche;
- invito alla programmazione dell'emissione della Carta nazionale dei servizi;
- realizzazione e promozione di servizi interattivi fruibili dagli utenti.

Si allega il testo:

Direttiva del 4 gennaio 2005
Linee guida in materia di digitalizzazione dell'Amministrazione

PREMESSA
La presente direttiva è indirizzata a tutte le Amministrazioni dello Stato e a tutti gli Enti pubblici sottoposti a vigilanza ministeriale. Per le Regioni e gli Enti locali costituisce contributo alle determinazioni in materia, nel rispetto della loro autonomia amministrativa, e sarà oggetto di successivo atto di indirizzo ai sensi dell'articolo 29, comma 7, della legge 23 dicembre 2001, n. 448 (legge finanziaria per il 2002).
Può rappresentare schema di riferimento anche per le altre amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165.
Le precedenti direttive e gli altri atti di indirizzo in materia di digitalizzazione, emanati anche in relazione a specifici settori, devono, comunque, intendersi validi ed efficaci e costituiscono parte integrante delle seguenti disposizioni.

1. STATO DI ATTUAZIONE DEGLI OBIETTIVI DI DIGITALIZZAZIONE

La rilevazione sullo stato di attuazione degli obiettivi di legislatura nella pubblica amministrazione ha evidenziato il raggiungimento di significativi risultati. Permangono, peraltro, disomogeneità tra le diverse amministrazioni.
In particolare si segnalano di seguito i principali risultati conseguiti e le maggiori criticità da affrontare:
a) circa il 50% dei servizi prioritari sono disponibili on-line, altri sono disponibili solo parzialmente. Per quelli rispetto ai quali si registrano criticità le Amministrazioni dovranno effettuare un'analisi puntuale dei motivi di ritardo, e produrre un piano al fine di accelerarne la realizzazione. E' in ogni caso opportuno attivare la verifica della soddisfazione dell'utente;
b) sono state distribuite oltre 1,6 milioni di carte di firma digitale. Il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) ha distribuito oltre 23.000 smart card ad altrettanti funzionari pubblici, con le quali vengono firmati digitalmente ogni giorno circa 3.000 mandati di pagamento. E' necessario rivedere le procedure amministrative al fine di estendere rapidamente l'utilizzo della firma digitale;
c) l'utilizzo della posta elettronica è sensibilmente aumentato nelle comunicazioni interne alla Pubblica Amministrazione. Poiché il completamento dell'Indice PA (elenco di tutti gli uffici pubblici con casella di posta elettronica a disposizione del pubblico), attualmente in corso di predisposizione ad opera del CNIPA, costituirà certamente un incentivo all'uso di tale strumento, si invitano le Amministrazioni che non abbiano ancora ottemperato all'invio dei dati ad attivarsi in tal senso con la massima urgenza garantendo, altresì, il tempestivo e costante aggiornamento dei dati stessi;
d) sempre nel settore della posta elettronica, va segnalato che molte amministrazioni hanno avviato iniziative per accrescere l'efficienza e ridurre i costi di proprie attività sostituendo ad operazioni materiali il ricorso a comunicazioni elettroniche.

In questo ambito si colloca anche l'iniziativa denominata @P@3, finalizzata a cofinanziare specifici progetti delle Amministrazioni. E' allo studio la possibilità di rilanciare il progetto per ulteriori iniziative di razionalizzazione e risparmi;
e) attualmente 25 milioni di impegni e mandati di pagamento sono on line. Nel corso del 2004 si è, infatti, esteso l'uso del Sicoge a quasi tutte le amministrazioni centrali (coprendo quasi il 100% dei capitoli di spesa delle stesse). Inoltre è stata automatizzata anche la gestione degli ordini di accreditamento che, a partire da giugno, comporta la gestione telematica di circa 175 mila ordini di accreditamento annuali; occorre però ancora estendere tali sistemi alle contabilità speciali;
f) le competenze informatiche acquisite dal personale pubblico sono molto diffuse; i dati sulla formazione a distanza (e-learning) indicano una crescita superiore al 60% sebbene permanga poco rilevante il numero delle certificazioni tipo ECDL o equivalenti;
g) l'accesso on-line all'iter delle pratiche mostra difficoltà legate al notevole impatto organizzativo. E' comunque in crescita la diffusione del protocollo informatizzato, prerequisito della trasparenza amministrativa. Nei settori nei quali è maggiore l'esigenza dei cittadini, ad es. fisco e previdenza, sono pienamente operativi call center utilizzabili anche per verificare lo stato delle pratiche e risolvere i problemi connessi. Per le Amministrazioni che non abbiano ancora completato l'automazione della gestione documentale e del protocollo informatico si segnala che il CNIPA propone tale servizio in modalità ASP 4;
h) non sono ancora presenti in tutti gli uffici i necessari strumenti di rilevazione della soddisfazione degli utenti.
Azioni conseguenti – Piani di recupero
Ogni Amministrazione dovrà verificare al proprio interno lo stato di attuazione degli obiettivi di legislatura, i motivi del mancato o parziale raggiungimento, e predisporre un Piano di recupero che ne consenta il conseguimento nei tempi stabiliti.
Detti Piani di recupero costituiranno parte integrante del Piano esecutivo per le tecnologie dell'informazione e della comunicazione (ICT) per il 2005 da trasmettere al CNIPA entro il 31 gennaio del 2005, redatto secondo le modalità stabilite al punto 6 della direttiva del 18 dicembre 2003.

2. LA SECONDA FASE DELLA DIGITALIZZAZIONE DELLA P.A.

Gli anni 2001-2004 hanno rappresentato la prima fase della digitalizzazione della Pubblica Amministrazione, nella quale l'impegno del Governo e delle amministrazioni è stato rivolto, soprattutto, al riorientamento ai servizi , allo sviluppo delle infrastrutture di base, alla diffusione di competenze informatiche e di una crescente familiarità con gli strumenti informatici tra i dipendenti e, nel periodo più recente, all' attivazione di siti web come canali di informazione ed in alcuni casi di erogazione di servizi on line agli utenti. In questa fase si è, quindi, pervenuti ad una maggiore diffusione, negli uffici e nei processi di lavoro, dell'uso delle ICT.
Le basi di questo importante processo di crescita sono state consapevolmente tracciate non solo e non tanto in disposizioni legislative, quanto – piuttosto – innescando un circuito virtuoso "definizione di obiettivi – attuazione – controllo" nelle amministrazioni, sostenuto anche attraverso il cofinanziamento di iniziative di innovazione proposte dalle stesse amministrazioni, sia centrali (attraverso deliberazioni del Comitato dei Ministri per la Società dell'Informazione) che locali (programma di e-Government).
Nel frattempo, come noto, sono stati disciplinati singoli strumenti e specifici istituti che connotano la digitalizzazione dell'Amministrazione (firma digitale, protocollo informatico, posta elettronica certificata, Carta di identità elettronica e Carta Nazionale dei Servizi, ecc.).
Questa prima importante fase della digitalizzazione della Pubblica Amministrazione può essere considerata conclusa. Infatti, sulla base del patrimonio di esperienze maturate, ha preso corpo la definizione di una nuova cornice normativa, che induce le amministrazioni a non adottare gli strumenti offerti dalle tecnologie dell'informazione e della comunicazione quali "possibilità aggiuntive" dell'azione amministrativa, ma a sostituire gli strumenti e le modalità tradizionali di rapporto con gli utenti e di svolgimento delle attività interne.

E' ora il momento di attivare la seconda fase, che dovrà essere improntata alla piena valorizzazione degli investimenti già realizzati, alla razionalizzazione del sistema nel suo complesso, alla interoperabilità tra le

amministrazioni, alla effettiva ed ampia transizione verso modalità di erogazione dei servizi on line e, infine, al raccordo pieno tra digitalizzazione, organizzazione, processi e servizi al pubblico.
Questo passaggio dalla prima alla seconda fase della digitalizzazione trova la sua cornice normativa nell'approvazione di due riforme organiche che costituiranno la base per l'evoluzione dell'e- Government nei prossimi anni.
La prima riforma è contenuta nel decreto legislativo sul Sistema Pubblico di Connettività e Cooperazione, ormai vicino alla definitiva adozione e che sostituirà, nello spirito di una visione pienamente condivisa tra Stato, Regioni ed Enti Locali, la Rete Unitaria delle Pubbliche Amministrazioni. Il nuovo sistema raccorderà tutte le pubbliche amministrazioni statali, regionali e locali.
La seconda riforma è costituita dal "Codice dell'Amministrazione digitale", che darà un assetto unitario ed organico al complesso di diritti dei cittadini e delle imprese, agli istituti giuridici ed ai doveri delle amministrazioni in materia di digitalizzazione delle pubbliche amministrazioni.
La prossima approvazione del decreto legislativo costituisce l'inizio di una seconda fase della digitalizzazione delle pubbliche amministrazioni, in quanto rende obbligatoria l'innovazione nella Pubblica Amministrazione nel modo più naturale: da una parte dando ai cittadini il diritto di interagire sempre, ovunque e verso qualunque amministrazione attraverso la rete; dall'altra, stabilendo che tutte le amministrazioni devono organizzarsi in modo da rendere sempre e comunque disponibili tutte le informazioni in modalità digitale.

Nuovi principi

I decreti legislativi concernenti il Sistema Pubblico di Connettività e Cooperazione (SPC) e il Codice dell'Amministrazione digitale forniranno l'adeguato supporto normativo in materia di dematerializzazione dei documenti, di comunicazione elettronica, di interazione a distanza, di circolarità e standardizzazione dei dati, di multicanalità, di accessibilità, di nuove competenze professionali.
In relazione a tali nuovi principi, le Amministrazioni pubbliche, anche con il supporto del CNIPA, dovranno, nel corso dell'anno 2005, porre in essere tutte le azioni di competenza per cogliere appieno le opportunità offerte dai nuovi strumenti.
In tale contesto, sarà necessario perseguire una piena integrazione degli interventi di digitalizzazione con le politiche di riforma delle pubbliche amministrazioni, con specifico riferimento alla semplificazione delle procedure e dell'organizzazione amministrativa ed alla formazione del personale. In particolare, le amministrazioni, nel programmare i loro interventi di digitalizzazione, dovranno segnalare al Dipartimento della funzione pubblica ed al Ministro per l'innovazione e le tecnologie sia le opportunità/necessità di semplificazione dei procedimenti amministrativi e delle regolamentazioni interne, sia i fabbisogni di nuove competenze, ai fini della adozione degli interventi conseguenti.

Settori di intervento

Le seguenti aree costituiscono settori di intervento essenziali alla realizzazione della seconda fase della digitalizzazione. Essi richiedono uno sforzo sinergico da parte delle singole Amministrazioni al fine di dare esecuzione alle azioni previste dalla normativa vigente e per la realizzazione delle quali il CNIPA ha impegnato le proprie risorse ed avviato le necessarie attività progettuali.

Comunicazione elettronica

Nel rammentare la direttiva concernente l'impiego della posta elettronica nelle pubbliche amministrazioni, nonché le norme relative all'utilizzo della firma digitale, si fa presente che sono di prossima definitiva approvazione le disposizioni necessarie per assicurare piena validità giuridica alle comunicazioni per via elettronica, sia all'interno di ciascuna amministrazione, sia tra amministrazioni diverse, sia, infine, tra amministrazioni, cittadini e imprese.
Di conseguenza diviene necessario riorganizzare il lavoro all'interno delle amministrazioni per sviluppare l'uso degli strumenti telematici, sostenendo minori oneri per la spedizione e l'archiviazione con notevoli vantaggi di velocità dell'azione amministrativa.

Rete Internazionale delle pubbliche amministrazioni

Per avvalersi dei previsti finanziamenti del CNIPA, le Amministrazioni che necessitano di connettività internazionale dovranno sottoscrivere i contratti di fornitura con l'aggiudicatario entro il primo trimestre del 2005.

Sistema Pubblico di Connettività e Cooperazione

Nelle more dell' attuazione del nuovo sistema, le Amministrazioni dovranno pianificare la migrazione dalla Rete Unitaria verso il nuovo Sistema Pubblico di Connettività e Cooperazione (SPC) presentando al CNIPA i relativi piani entro il 2005, al fine di non superare il termine di sei mesi dalla data del contratto quadro che sarà stipulato dal CNIPA.
Carta Nazionale dei Servizi (CNS)

Sono ormai definite con decreto dei Ministri dell'Interno, per l'innovazione e tecnologie, dell'economia e delle finanze, datato 9 dicembre 2004, 8 le regole tecniche sulla CNS; le amministrazioni dovranno, pertanto, programmare l'emissione della CNS in sostituzione di altri strumenti di accesso ai servizi sino ad ora realizzati, tenendo comunque presente che, ai sensi della normativa vigente, ogni Amministrazione deve, comunque, garantire l'accesso ai propri servizi da parte dei titolari di CNS.
Al fine di promuoverne la diffusione il CNIPA definirà un contratto quadro per la fornitura di CNS al quale le pubbliche amministrazioni potranno aderire.

Servizi on line agli utenti

Si conferma la priorità di favorire la diffusione e l'utilizzo di servizi on line per cittadini ed imprese, per migliorare il servizio e ridurre i costi. Le amministrazioni dovranno, pertanto, curare la realizzazione e la promozione di servizi interattivi, assicurando, nel contempo, la possibilità di accesso attraverso una pluralità di canali (internet, telefonia mobile, telefonia fissa, tv digitale), ciascuno facoltativamente fruibile dagli utenti.
In tale ottica le amministrazioni dovranno collaborare per integrare i procedimenti di rispettiva competenza, al fine di agevolare gli adempimenti richiesti alle imprese e accrescere l'efficienza nelle aree che coinvolgono più amministrazioni, attraverso la definizione e l'attuazione di accordi per la partecipazione al sistema di cooperazione attuato nell'ambito del Sistema per i servizi integrati alle imprese (www.impresa.gov.it).

Gestione documentale

Le amministrazioni dovranno porre in atto tutte le misure previste dalla normativa in materia di gestione documentale eventualmente avvalendosi dei servizi resi disponibili dal CNIPA nell'ambito dell'iniziativa Servizio di gestione del Protocollo Informatico e gestione documentale in modalità ASP.

3. RISPARMI e RAZIONALIZZAZIONE

L'articolo 1, commi da 192 a 196, della legge finanziaria per il 2005, introduce nuovi modelli di comportamento per le pubbliche amministrazioni finalizzati alla razionalizzazione dei processi operativi e, conseguentemente, al contenimento della spesa.
La sua attuazione avverrà attraverso l'emanazione di successivi DPCM che individueranno le aree prioritarie e l'ambito soggettivo di intervento, al fine di predisporre un programma strutturale per l'informatica pubblica e la sua contestuale razionalizzazione, mantenendo l'attuale impulso all'innovazione, accelerando lo sviluppo e la diffusione di soluzioni tecnologiche e organizzative innovative, evitando, altresì, che questo sviluppo si traduca in incremento della spesa informatica e, al contrario, producendo economie.
Ciò sarà possibile utilizzando le nuove modalità di approvvigionamento dei servizi che semplificano le incombenze delle singole amministrazioni, anche assumendo come modello di riferimento quello dei servizi ASP.

Per la migliore attuazione della nuova disciplina introdotta dalla legge finanziariaè auspicabile un'attiva collaborazione con il CNIPA da parte delle Amministrazioni che potranno contribuire a determinarne gli ambiti di azione, effettuando una accurata analisi della propria situazione in rapporto all'utilizzo delle ICT al fine di individuare:
- i casi di duplicazione o ridondanza di sistemi e strutture informatiche, sui quali sia possibile intervenire per razionalizzare e conseguire economie gestionali;
- i casi in cui sia possibile ed opportuno utilizzare soluzioni condivise o soluzioni già adottate in altre amministrazioni.
E' da sottolineare la possibilità di conseguire economie anche attraverso l'applicazione della Direttiva inerente l'acquisizione del software, da effettuarsi attraverso una valutazione comparativa che tenga anche conto di prodotti disponibili in riuso od a codice sorgente aperto. E' all'uopo disponibile una proposta di metodologia di valutazione messa a punto dal CNIPA.
Nell'ambito delle iniziative tendenti alla razionalizzazione ed al risparmio, particolare importanza assume l'adozione della tecnologia "Voice over IP", che consente di trasportare le conversazioni vocali via Internet o su reti per trasmissione dati che operano in modo analogo ad Internet, impiegando router e server di rete in luogo di centrali telefoniche e centralini. I centralini, pertanto, vengono sostituiti da server, utilizzando, di norma, il cablaggio esistente ed eliminando così costose duplicazioni.
L'adozione di questa tecnologia consente di ricorrere ad un collegamento unico per qualsiasi tipo di comunicazione (voce, dati e immagini), attraverso il Sistema Pubblico di Connettività e la Rete Internazionale delle Pubbliche Amministrazioni, che sono state progettate per un trasporto di qualità per ciascuna delle indicate tipologie di comunicazioni. I vantaggi concreti potenzialmente derivanti dall'adozione del Voip consistono in una notevole riduzione delle spese di telefonia, oltre che delle spese di gestione e manutenzione, a parità di qualità del servizio, grazie :
- all'azzeramento dei costi delle conversazioni all'interno delle amministrazioni nonché alla riduzione dei costi delle chiamate verso l'esterno;
- alla riduzione dei costi di gestione per l'impiego di un unico cablaggio e di impianti della stessa tipologia per voce e dati;
- all'azzeramento dei costi legati agli spostamenti delle connessioni telefoniche del personale che possono essere realizzati con un semplice comando via software.
Le Pubbliche Amministrazioni con contratti in scadenza a breve in questo settore dovranno valutare, prima del rinnovo dei contratti stessi, la convenienza del passaggio alle nuove tecnologie, anche avvalendosi dell'apposito Centro di Competenza, all'uopo istituito presso il CNIPA che potrà fornire, anche, supporto alla pianificazione dell'introduzione della tecnologia Voip ed alla sostituzione degli impianti esistenti, da programmare nell'arco di tre anni.

4. RUOLO DELLA DIRIGENZA

Per la realizzazione dei citati obiettivi e per il successo della seconda fase di digitalizzazione dell'Amministrazione, appare necessario il più ampio coinvolgimento dei dirigenti ai quali dovranno essere, conseguentemente, assegnati corrispondenti obiettivi da realizzare nel corso dell'anno.
Tale coinvolgimento dovrà mirare ad ottenere, da parte della dirigenza, non soltanto il raggiungimento degli obiettivi prefissati, ma anche a suscitare un atteggiamento propositivo per la definizione dei programmi strategici delle singole Amministrazioni.
Ogni dirigente di vertice delle strutture in cui si articola ciascuna amministrazione dovrà essere responsabilizzato per la definizione e per il raggiungimento di precisi obiettivi nei settori indicati dalla presente direttiva, indicando i conseguenti risparmi e le esigenze di formazione del personale.
Appare, infatti, indispensabile curare che, attraverso un adeguato programma di formazione tecnica, giuridica e organizzativa, sia assicurato un livello di conoscenza tale da porre la dirigenza in condizione di essere essa stessa motore del cambiamento in atto nell'agire dell'Amministrazione.

Sentenza del T.A.R. Lazio sull'inserimento di provvedimenti amministrativi su sito Internet.

NUMERO SCHEDA: 5027

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: TAR LAZIO

NATURA ATTO: SENTENZA

DATA ATTO: 04/11/2003

NUM. ATTO: 9430

ORGANO: TAR LAZIO

Secondo il T.A.R. Lazio dalla mancata partecipazione ad un procedimento illegittimo non può discendere una preclusione per la tutela degli interessi di chi lamenta una diretta ed immediata lesione della sua sfera patrimoniale.
Inserire su di un sito Internet alcuni provvedimenti amministrativi non è considerato dalla legge uno strumento idoneo ad assicurare la conoscenza legale degli stessi. Esso ha esclusivamente valore di pubblicità notizia.

Si allega copia della sentenza del T.A.R. Lazio, Sez. III ter del 4 Novembre 2003, n. 9430.

S E N T E N Z A

FATTO

Con il presente gravame, l'ENEL Distribuzione ricorrente impugna la concessione dell'attività di distribuzione di energia elettrica per i comuni di NoIa (Na) e Casamarciano alla controinteressata SNIE S.p.a. denunciando due motivi di gravame relativi alla violazione dell'art. 9 commi 3 e 4 del D.lgs. n. 79/1999; ed all'eccesso di potere sotto diversi profili.
La controinteressata,formalmente costituitasi in giudizio il 14 gennaio 2003, con analitica memoria ha confutato le argomentazioni di ricorso e, invocando alcuni precedenti in sede cautelare della Sezione, ha concluso per il rigetto.
Il Ministero, costituitosi in giudizio il 14 gennaio 2003, in data 15 settembre 2003 ha versato alcuni atti del procedimento.
Con memoria del 27 settembre 2003, la difesa del ricorrente ha sottolineato le tesi a sostegno delle proprie argomentazioni.
Con scritti difensivi in data 28 settembre 2003 la Difesa Erariale ha contestato la affermazioni di cui al ricorso ed ha concluso per il rigetto.
All'udienza del 9 ottobre 2003 la difesa dell'ENEL, con l'assenso delle controparti, depositava copia della convenzione-quadro di concessione dell'attività tra il M.A.P. e l'Enel Distribuzione; e chiedeva l'acquisizione del D.M. contenente i "criteri indicativi" per la individuazione delle percentuali delle utenze rilevanti al fine della prevalenza in ciascun Comune, già firmato ed in corso di emanazione.

I patrocinatori della controinteressata si opponevano alla richiesta istruttoria eccependo l'estraneità del predetto decreto al presente contendere, ed insistevano per il passaggio in decisione.
La causa è stata a tal fine trattenuta dal Collegio.

D I R I T T O

1. Devono essere preliminarmente confutate le eccezioni preliminari introdotte dalla difesa della controinteressata.

1.1. La controinteressata eccepisce in primo luogo che la ricorrente società "Enel Distribuzione" s.p.a. -- che peraltro nei comuni serviti in via esclusiva (100%) sarebbe un concessionario in *prorogatio* essendo scaduto il 31 marzo 1999 il decreto di concessione -- non sarebbe legittimata alla proposizione del presente ricorso perché non avrebbe presentato nel termine fissato dal D.L.gs. n. 79/1999 la specifica domanda di rilascio di concessione relativamente ai Comuni di Noìa e di Casamarciano. Avendo definitivamente perso il titolo all'esercizio dell'attività, l'ENEL non potrebbe affatto sindacare gli esiti di una procedura alla quale è rimasta estranea (cfr. Cons. Stato, sez. V, 17 gennaio 2002 n.253, 3 gennaio 2002 n.6, 5 settembre 2002 n. 4458).
L'eccezione va respinta.
Si deve puntualizzare in punto di fatto che l'Enel Distribuzione, con la nota del 3.3.2000 e protocollata dal Ministero in data 10 aprile 2000, aveva effettuato la richiesta di concessione per tutti i Comuni serviti in via esclusiva. Nella medesima istanza l'Enel si era riservata -- relativamente ai Comuni serviti in via promiscua (come nel caso di Nola e Casamarciano) -- di effettuare le "*singole proposte di aggregazione*" con le aziende distributrici via via che sarebbero state perfezionate con le diverse aziende elettriche minori le trattative commerciali previste dall'art. 9 del d.lgs. n. 79/1999.
Non vi era dunque alcun bando e alcuna norma che obbligasse l'ENEL a fare una richiesta a pena di decadenza, in quanto la disciplina per il rilascio delle concessioni in questione prevedeva uno sviluppo procedimentale affatto diverso da quello seguito nel caso di specie dall'Amministrazione.
In conclusione sul punto, dalla mancata partecipazione ad un procedimento illegittimo non può certo discendere una preclusione per la tutela degli interessi di chi lamenta una diretta ed immediata lesione della sua sfera patrimoniale.
Non vi sono dubbi dunque circa la sussistenza di un interesse giuridicamente protetto della società ricorrente alla rimozione del provvedimento impugnato.

1.2. Parimenti inconsistente è poi l'eccezione di tardività.
Per la controinteressata, la piena conoscenza della concessione si sarebbe verificata al momento della pubblicazione sul sito del Ministero il 2 agosto 2002. Il gravame, notificato il 2 dicembre 2002, sarebbe dunque tardivo in quanto introdotto quando era già decorso il termine decadenziale.
Per contro si osserva che l'inserimento in sito Internet di provvedimenti amministrativi non è elevato dalla legge a strumento diretto ad assicurare la legale conoscenza degli atti amministrativi, per cui la pubblicazione di atti amministrativi in Internet ha valore di pubblicità notizia (cfr. T.A.R. Lazio, sez. II, 13 marzo 2001, n. 1853).
Pertanto, non può farsi luogo a presunzioni di sorta ed il ricorso deve essere ritenuto pienamente ammissibile non essendo stata fornita dalla controinteressata la prova di una effettiva conoscenza anteriormente alla pubblicazione sulla Gazzetta Ufficiale.

1.3 Infine si eccepisce l'inammissibilità del ricorso per l'omessa impugnativa del parere dell'Autorità per l'energia ed il Gas n.37/01 e del parere dell'Autorità garante della Concorrenza dell'aprile 2001. Essendo pareri obbligatori, avrebbero dovuto essere espressamente impugnati non potendo valere a tal fine la generica formulazione di stile dell'impugnativa di "tutti gli atti presupposti".
L'eccezione è priva di pregio.
Nel caso in esame la lesione è esclusivamente dovuta al provvedimento e, non a caso, nemmeno la controinteressata riesce ad indicare quale sarebbe l'elemento concreto dei pareri che, essendo immediatamente ed autonomamente lesivo per la posizione giuridica della ricorrente, avrebbe richiesto una immediata impugnativa.
I due pareri in questione (obbligatori ma non vincolanti) nello specifico caso concernevano i profili generali delle convenzioni e dei connessi procedimenti.
In ogni caso dal loro contenuto non è dato riconnettere alcuna preclusione processuale per il presente ricorso. Di qui la piena ammissibilità del gravame anche sotto tale punto di vista.

2. Nel merito il ricorso è fondato per l'assorbente considerazione del primo motivo.

L'Enel Distribuzione Spa deduce l'illegittimità del decreto con cui il Ministero delle Attività produttive ha rilasciato la "concessione unica", per la distribuzione di energia elettrica per i comuni di Nola e Casamarciano (Na) alla controinteressata SNIE S.p.a. per violazione dell'art. 9, III° co. del D.lgs. n. 79/1999.
In particolare la Società ricorrente lamenta:
-- l'insuscettibilità di applicazione analogica del quarto comma dell'art. 9 del D.lgs. n. 79/1999, che prevede la possibilità delle sole Società di distribuzione partecipate dagli EE.LL. che raggiungono almeno il 20 % delle utenze di chiedere all'ENEL la cessione dei rami d'azienda dedicati all'esercizio dell'attività di distribuzione, alle altre società. Per la ricorrente si tratterebbe di una norma assolutamente e pacificamente di carattere eccezionale volta a valorizzare le partecipazioni degli enti locali;
-- il provvedimento non sarebbe stato preceduto da alcuna valutazione comparativa e non avrebbe offerto alcuna ragionevole e fondata motivazione;
-- il Ministero avrebbe violato i principi di equità, ragionevolezza e parità di trattamento in quanto una presenza nel Comune di Nola del 29% non poteva ritenersi più significativa della presenza del 71 % di utenze detenute dall'ENEL.
-- la concessione avrebbe invece dovuto tener conto del criterio della "significativa partecipazione, anche quantitativa, sul territorio di un'effettiva rete di distribuzione";
L'assunto merita adesione nei sensi che seguono.
I° Sotto il profilo sostanziale si osserva che la impugnata concessione viola il paradigma normativo che disciplina l'assegnazione delle concessione alle imprese elettriche di cui all'art. 9 del D.lgs. n. 79 del 16 marzo 1999. In particolare il provvedimento è ancorato:
a.1) alla sussistenza di una domanda della SNIE;
b.1) alla generica considerazione che la SNIE avrebbe una "*presenza significativa anche in termini quantitativi*" per cui quest'ultima sarebbe "*un soggetto idoneo*";
c.1) al perseguimento "*dell'obbiettivo di valorizzare le imprese distributrici diverse dall'ENEL per promuovere il pluralismo dell'offerta*".
Al riguardo di tali elementi si osserva in dettaglio quanto segue.
a.2) Quanto al riferimento alla "*domanda della SNIE*", il terzo comma dell'art. 9 del D.lgs. cit., non contiene alcuna disposizione che -- nei comuni, ove alla data di entrata in vigore del medesimo decreto, operavano più distributori -- potesse consentire al Ministero di delibare autonomamente sulle richieste di singole aziende elettriche.
Al contrario anzi la predetta norma dispone che i diversi soggetti imprenditoriali compresenti nei medesimi ambiti in via ordinaria "*attraverso le normali regole di mercato, adottano le opportune iniziative* per la loro aggregazione e sottopongono per approvazione le relative proposte" al Ministro dell'industria, del commercio e dell'artigianato entro il 31 marzo 2000.
In altre parole, nei casi di servizi promiscuamente forniti da più società nei medesimi Comuni, le imprese private elettriche aspiranti a subentrare all'ENEL distribuzione S.p.a. avrebbero dovuto trovare un accordo industriale ed economico con l'ex Ente Nazionale.
In difetto del perfezionamento di tale accordo, il Ministro dell'Industria (oggi delle Attività Produttive) con il Ministro del Tesoro (oggi dell'Economia) avrebbe dovuto promuovere la predetta aggregazione, "*anche attraverso specifici accordi di programma*".
Pertanto, anche nel caso di difficoltà di accordo, la norma prevede un'aggregazione, su base consensuale.
Contrariamente a quanto mostra di ritenere la Difesa Erariale, quindi non è assolutamente previsto un potere discrezionale del Ministero di assegnare direttamente la concessione per la distribuzione le reti.
Un tale potere si risolverebbe in una immotivata concessione di una posizione economica di rilevante profilo, al di fuori di ogni norma e senza nemmeno un serio corrispettivo.
Essendo l'Enel una società privata con una consistente quota di azioni collocate sul libero mercato, per poter procedere all'adozione di provvedimenti di espropriazione forzata dei suoi diritti e delle sue proprietà, sarebbe stata necessaria una disposizione di legge *ad hoc*. Il che non è.
Anche facendo riferimento alla fattispecie di cui quarto comma dell'art. 9 del d.lgs. n.79, il richiamo alla domanda della SNIE è comunque giuridicamente inconferente.
Il predetto comma disciplina la differente ipotesi, di carattere eccezionale e suppletivo, per cui, nei casi in cui non sia stato possibile accedere agli accorpamenti di cui al terzo comma, "*le società di*

distribuzione partecipate dagli enti locali" senza distinzione di dimensioni possono "*chiedere all'ENEL S.p.a. la cessione dei rami d'azienda dedicati all'esercizio dell'attività di distribuzione nei comuni nei quali le predette società servono almeno il venti per cento delle utenze*".
Tale disposizione, non disciplina infatti la concessione alle aziende elettriche minori di proprietà privata, e comunque prevede un'istanza all'Enel -- e non al Ministero-- dalla quale può solo scaturire un'accordo convenzionale.
In realtà, l'unica disposizione che prevede un'istanza diretta al Ministero dell'Industria, è quella del V° comma dell'art. 9 concernente l'ulteriore caso in cui "le società degli enti locali aventi non meno di 100.000 clienti finali", potevano richiedere al Ministro dell'industria, del commercio e dell'artigianato "di avvalersi delle procedure di cui al medesimo comma 3" relativamente ad ambiti territoriali contigui, entro un anno dalla data di entrata in vigore del D.lgs. n.79/99. Ma tale disposizione in favore delle imprese degli Enti locali, appare legittimamente introdotta per la fondamentale considerazione che si tratta di imprese pubbliche di lunga tradizione imprenditoriale, sociale ed economica.
Ma anche in questo caso la norma prevedeva l'istanza al Ministro dell'industria, per l'ammissione alla procedura (in esito della quale l'Enel era obbligata a trattare) ma non la possibilità del Ministero di far luogo direttamente alla concessione.
Entrambe le disposizioni fanno esclusivo riferimento alle imprese pubbliche degli EE.LL e non alle imprese di proprietà privata, autorizzate a proseguire l'attività di distribuzione dell'energia elettrica ai sensi della L. n. 10/1991.
In definitiva l'analisi complessiva dell'art. 9 del D.lgs. n.79/1999 porta a concludere per l'inesistenza di un potere del Ministero di assegnare discrezionalmente le concessioni in assenza di un accordo con l'ENEL .
E tale conclusione appare perfettamente speculare alla disciplina della direttiva 96/92/CE la quale, relativamente alla fase di distribuzione dell'energia elettrica, era programmaticamente imperniata:
-- sul fatto che il mercato avrebbe dovuto "…. essere instaurato *progressivamente* al fine di consentire all'industria di adeguarsi in modo flessibile e composto al suo nuovo contesto e per tener conto dei diversi modi nei quali le reti elettriche sono attualmente organizzate …"(così il 5° *considerando*);
-- sulla necessità che, in ogni caso i processi di privatizzazioni dovessero evitare "*ogni abuso di posizione dominante e ogni comportamento predatorio* (così il 37° *considerando*) da parte dei nuovi gestori privati nei riguardi dell'utenza onde impedire che il frazionamento degli enti distributori si risolvesse in un mero aggravio dei costi per il pubblico ed in un aumento dei disservizi a cagione delle scelte di politica industriale delle aziende distributrici (specie riguardo alla manutenzione delle reti) particolarmente mirate al profitto.

b.2) Parimenti del tutto incongruente con la norma dell'art. 9 è il riferimento alla "*presenza significativa anche in termini quantitativi*" della SNIE, da cui il provvedimento fa apoditticamente discendere la conclusione che la stessa fosse "*un soggetto idoneo".*
Come visto, il quadro normativo dell'art. 9, non fa alcuna questione nè di prevalenza né di idoneità tecnica dell'impresa a diventare concessionaria unica.
Questi fattori non sono assolutamente presi in considerazione a proposito delle aziende elettriche minori, per cui non potevano assolutamente giustificare sul piano giuridico il provvedimento.
In ogni caso, sul piano logico, il meccanicistico collegamento, tra la rilevanza delle utenze e la qualificazione della SNIE quale un "soggetto idoneo", non solo è una *consecutio* arbitraria, ma comunque si risolve in una conclusione assolutamente apodittica, non essendo stata effettuata alcuna ogni indagine istruttoria al riguardo.
In ogni caso, il concetto di "significativa presenza" non poteva portare a far ritenere prevalente la posizione del soggetto che, nel Comune di Nola, aveva il 29 % e soccombente quella di chi aveva il 71 %..
A tutto voler concedere, anche il lodevole intento di favorire il pluralismo delle imprese (peraltro giudicato "*prima facie*" legittimo dalla sezione per le partecipate dagli enti locali) finisce per diventare, nel caso in esame, del tutto illogico e manifestamente iniquo in relazione alla consistenza delle reciproche utenze.
In definitiva sul punto, il rilievo alla presenza della SNIE non poteva supportare alcuna *potioretà* nell'affidamento della concessione in quanto era un elemento non previsto dall'art. 9 del d.lgs. cit. .

c.2) Di conseguenza si deve anche concludere che il perseguimento "*dell'obbiettivo di valorizzare le imprese distributrici diverse dall'ENEL per promuovere il pluralismo dell'offerta*", genericamente affermato dal provvedimento era giuridicamente del tutto inappropriato.
La "significativa" presenza non poteva avere alcun rilievo giuridico in quanto l'unico riferimento al "*mantenimento del pluralismo nell'offerta di servizi e del rafforzamento di soggetti imprenditoriali anche nella prospettiva dell'estensione del mercato della distribuzione"*, è contenuta nel ricordato quarto comma dell'art. 9 del cit. d.lgs. con riferimento alle sole imprese partecipate dagli enti locali ma non le imprese elettriche private.
Né poteva farsi alcuna estensione analogica delle norme di cui ai commi quattro e cinque del cit. art. 9, che erano esclusivamente previste per le imprese elettriche minori (essendo al riguardo gli Ordini del Giorno parlamentari invocati dei meri atti di auspicio).
In ogni caso l'affermazione del provvedimento sul pluralismo aziendale appare assolutamente enfatica perché, ai processi di "liberalizzazione" della distribuzione di energia elettrica non consegue la reale possibilità dell'utente privato di scegliere fra più gestori.
La realizzazione dei processi di "privatizzazione", risolvendosi solamente in un ulteriore frazionamento delle aziende distributrici sul territorio, non implicava dunque che la concessione per la distribuzione dovesse necessariamente e pregiudizialmente spettare all'impresa elettrica minore.
In definitiva, il D.lgs. n. 79/1999 non conferisce al Ministro alcun potere discrezionale di conferire la concessione alle imprese elettriche private, al di fuori delle iniziative di accorpamento da concordare con l'Enel ai sensi del terzo comma dell'art. 9; e non prevede forme, neanche indirette, di espropriazione di fatto di diritti a favore di imprenditori privati.
Non vi sono, in ogni caso, dubbi sulla illegittimità del provvedimento impugnato, per violazione dell'art. 9 del D.lgs. n. 79.

II° Sul piano procedimentale la concessione impugnata è comunque illegittima per eccesso di potere per difetto di motivazione, errore sui presupposti, illogicità e sviamento.
La motivazione del provvedimento ministeriale non dà infatti alcuna indicazione sui reali presupposti di diritto e di fatto che avrebbero indotto il Ministro a privilegiare la controinteressata SNIE in danno dell'ENEL.
Anche alla luce delle considerazioni del punto che precede, il difetto di motivazione del provvedimento non ha un rilievo meramente formale ma appare sintomaticamente rivelatore di un vizio funzionale del provvedimento, per il mancato rispetto dei precetti della logica, della coerenza interna e razionalità.
In primo luogo, la lontananza con lo schema legale del procedimento quale era disegnato dalla norma, è significativamente rivelata e dimostrata anche dal fatto che il provvedimento si limita a richiamare del tutto genericamente l'art. 9 del D.lgs. n.79/1999, senza preoccuparsi di specificare esattamente il comma del quale si sarebbe fatto applicazione nella specie.
In secondo luogo, risulta dalle stesse allegazioni della controinteressata, che la SNIE aveva fatto domanda per tutti gli otto Comuni nei quali operava: al riguardo non si comprende nemmeno perché il provvedimento abbia abbinato solo i due Comuni più popolosi (di Nola e Casamarciano), e abbia del tutto omesso ogni riferimento a proposito degli altri sei Comuni per i quali risulta che l'Azienda aveva pure fatto "istanza" al Ministero.
In terzo luogo è evidente come, di fronte a due situazioni di interesse speculatmente contrapposte, l'Amministrazione non abbia assolutamente fatto luogo ad una bilanciata ed imparziale comparazione, tra la posizione dell'ENEL e quella della SNIE.
In quarto luogo, fuorviante appare il generico richiamo "Vista la *proposta dell'Autorità per l'energia elettrica ed il gas di cui alla delibera d. 37/01*".
L'allocuzione, posta maniera del tutto indeterminata e senza ulteriori specificazioni, sembra quasi voler far intendere che la specifica determinazione di assegnare alla SNIE la concessione derivasse da una proposta dell'Autorità. Il che non è perchè, come già rilevato, la delibera citata conteneva il parere generale sullo schema delle concessioni ai sensi del d.lgs. n. 79/1999.

3. In conclusione il ricorso è fondato, e per l'effetto deve essere pronunciato l'annullamento del provvedimento impugnato.
Sussistono tuttavia, in relazione alla novità della materia, sufficienti motivi per disporre l'integrale compensazione delle spese del presente giudizio.
P.Q.M.

il Tribunale Amministrativo Regionale del Lazio – Sez. III^-ter :
1) accoglie il ricorso n. 13883/2002 e per l'effetto annulla il provvedimento di cui in epigrafe.
2) Spese compensate.
Ordina che la presente sentenza sia eseguita dall'Autorità Amministrativa.
Così deciso dal Tribunale Amministrativo Regionale del Lazio – Sez. III^-ter, in Roma, nella Camera di Consiglio del 9 ottobre 2003.

Sono Stati creati i Centri regionali di competenza nell'ambito della strategia di cooperazione tra i livelli di governo coinvolti nell'e.government.

NUMERO SCHEDA: 4637

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE:

FONTE: IL SOLE 24 ORE

DATA: 30/04/2004

PAGINA: 7

NATURA ATTO: COMMENTO

Il Dipartimento per l'innovazione e le Tecnologie, d'intesa con il Dipartimento della Funzione Pubblica e con il supporto operativo del Formez, ha realizzato il progetto Centri Regionali di competenza per l'e-government e la Società dell'Informazione.In particolare, ciascun CRC è costituito sulla base di apposite convenzioni tra il Ministro per l'innovazione e le Tecnologie e i presidenti delle Regioni.
Il CRC è una struttura composta da operatori dei diversi livelli del governo regionale e locale che ha la finalità di affiancare e facilitare l'azione delle Autonomie Locali tesa ad innovare i servizi ed a sviluppare i piani e i progetti di e-government.
Si tratta di strutture snelle ed operative ubicate sul territorio regionale che hanno il ruolo di facilitare l'attuazione dei processi di innovazione attraverso la realizzazione di piani di attività formative, informative e di assistenza agli Enti Locali.
Ciascun centro sviluppa un piano di attività con modalità operative e finalità proprie, adeguate alle esigenze della realtà locale, e, al tempo stesso, è in rete con gli altri centri regionali e beneficia di servizi e supporti comuni.
Gli obiettivi del progetto si possono sintetizzare nel seguente modo:

- sviluppare la cooperazione tra il Dipartimento per l'Innovazione e le Tecnologie e i sistemi regionali, mettendo in rete i CRC in un network nazionale, rappresentativo del nuovo assetto istituzionale federalista e supportando la Commissione Permanente sull'Innovazione e le Tecnologie;
- supportare gli Enti Locali e rafforzarne le competenze nella definizione ed attuazione di programmi e progetti per l'e-government e la Società dell'Informazione, in coerenza con gli obiettivi fissati dalle Linee Guida del governo;

- definire e diffondere modelli, approcci e strumenti condivisi e integrati sugli aspetti critici della realizzazione dei processi di innovazione;
- sviluppare la cooperazione ed il coordinamento tra diversi livelli di governo nei sistemi regionali e favorire scambi e azioni comuni su scala interregionale.

I Centri attivi sono 20 (Liguria, Calabria, Emilia Romagna, Friuli - Venezia Giulia, Sicilia, Basilicata, Marche, Puglia, Toscana, Veneto, Umbria, Sardegna, Lombardia, Campania, Abruzzo, Piemonte, Valle d'Aosta, Provincia Autonoma di Trento, Provincia Autonoma di Bolzano e Lazio).

Contesto, motivazioni e obiettivi dell'intervento per la creazione dei Centri Regionali di Competenza sono contenuti nel "Progetto per una rete di Centri Regionali di Competenza per l'e-government nelle regioni italiane".

Appalti P.A. con firma digitale e senza la documentazione cartacea. La Consip offre alle imprese che partecipano alle sue gare d'appalto la possibilità di partecipare con documentazione digitale.

NUMERO SCHEDA: 4522

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: ITALIA OGGI

AUTORE: Chiara CINTI

DATA: 24/03/2004

PAGINA: 29

NATURA ATTO: COMMENTO

Per la prima volta in Italia la Consip offre la possibilità di effettuare gare di appalti con documentazione di gara e offerte su cd-rom, anziché in forma cartacea. L'inaugurazione di questo nuovo sistema sarà il pubblico incanto per la fornitura di hardware e software di base e servizi per il progetto "Nuovo Spt – sistema per la gestione dei pagamenti al personale della pubblica amministrazione" del ministero dell'economia e delle finanze. Con questa procedura si avrà un risparmio di tempo e carta e si riducono i margini di errore; inoltre diminuiranno grazie ai cd-rom i problemi di conservazione dei documenti d'offerta, sarà più difficile smarrire quelli relative alle gare. I documenti potranno essere consegnati su supporto ottico, naturalmente senza nulla togliere alla documentazione prodotta in forma cartacea.
Inoltre, si segnala che, il centro nazionale per l'informatica nella pubblica amministrazione (Cnipa) ha pubblicato sulla Gazzetta Ufficiale n. 57 del 09/03/2004

serie generale, la circolare n. 11/2004 che ha sostituito integralmente la circolare n. 42 del 13/12/2001 dell'Aipa. La circolare, consultabile sul sito internet www.gazzettaufficiale.it, tratta l'adeguamento delle procedure informatiche della pubblica amministrazione alle più recenti tecnologie informatiche e detta nuove regole per la conservazione sostitutiva dei documenti informatici.

Il Centro nazionale per l'informatica nella pubblica amministrazione modifica le regole per la riproduzione e la conservazione dei documenti su supporto ottico.

NUMERO SCHEDA: 4484

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: WWW.CITTADINOLEX.IT

NUMERO: 57

DATA: 09/03/2004

NATURA ATTO: DELIBERA

NUM. ATTO: 11

Con deliberazione n.11/2004 il Centro nazionale per l'informatica nella pubblica amministrazione modifica le regole per la riproduzione e la conservazione dei documenti su supporto ottico, nell'ottica di un adeguamento programmato delle procedure operative rispetto all'evolversi continuo delle tecnologie.
Il CNIPA aveva già rilevato alcuni problemi nel primitivo regolamento concernente l'argomento (cioè la delibera AIPA n. 42/2001), riguardanti sia aspetti pratici e gestionali del sistema di archiviazione, sia nello specifico dei campi di competenza precisati nelle definizioni (articolo 1).
Riguardo al primo aspetto il CNIPA aveva rilevato che la tecnologia suggerita per la firma del file dei documenti da conservare era attuabile solo per quelli di dimensioni molto piccole. Pertanto era stato variato sostanzialmente l'articolo 3, che nel vecchio regolamento si occupava in forma generica di archiviazione di documenti analogici e che nel nuovo, invece, concerne quelli informatici.
Il secondo aspetto ha investito una riformulazione delle definizioni (contenute nell'articolo 1) relative al "documento informatico" ed alla "firma digitale" (questa ultima in particolare non era presente nella deliberazione citata), poiché esse non erano coerenti con quelle presenti nel Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (DPR n.445/2000), a seguito del recepimento della direttiva comunitaria sulla firma digitale.

Inoltre, l'articolo 1 è stato ulteriormente ampliato con definizioni concernenti l'evidenza informatica, l'impronta e la funzione di hash (una tecnica per impedire manipolazioni informatiche).

Si riporta di seguito il testo della deliberazione.

CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE.
DELIBERAZIONE 19 febbraio 2004.

Art. 1.
Definizioni

Ai fini della presente deliberazione si intende per:
a) documento: rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica;
b) documento analogico: documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia;
c) documento analogico originale: documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;
d) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
e) supporto ottico di memorizzazione: mezzo fisico che consente la memorizzazione di documenti informatici mediante l'impiego della tecnologia laser (quali, ad esempio, dischi ottici, magneto-ottici, DVD);
f) memorizzazione: processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti ai sensi dell'art. 10, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, così come modificato dall'art. 6 del decreto legislativo 23 gennaio 2002, n. 10 [2];
g) archiviazione elettronica: processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, così come individuati nella precedente lettera f), univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione;
h) documento archiviato: documento informatico, anche sottoscritto, così come individuato nella precedente lettera f), sottoposto al processo di archiviazione elettronica;
i) conservazione sostitutiva: processo effettuato con le modalità di cui agli articoli 3 e 4 della presente deliberazione;
l) documento conservato: documento sottoposto al processo di conservazione sostitutiva;
m) esibizione: operazione che consente di visualizzare un documento conservato e di ottenerne copia;
n) riversamento diretto: processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, non alterando la loro rappresentazione informatica. Per tale processo non sono previste particolari modalità;
o) riversamento sostitutivo: processo che trasferisce uno o più documenti conservati da un supporto ottico di memorizzazione ad un altro, modificando la loro rappresentazione informatica. Per tale processo sono previste le modalità descritte nell'art. 3, comma 2, e nell'art. 4, comma 4, della presente deliberazione;
p) riferimento temporale: informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici;
q) pubblico ufficiale: il notaio, salvo quanto previsto dall'art. 5, comma 4 della presente deliberazione e nei casi per i quali possono essere chiamate in causa le altre figure previste dall'art. 18, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
r) evidenza informatica: una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica;
s) impronta: la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash;

t) funzione di hash: una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali;
u) firma digitale: così come definita all'art. 1, comma 1, lettera n), del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 [3].

Art. 2.

Obblighi di conservazione sostitutiva

1. Gli obblighi di conservazione sostitutiva dei documenti, previsti dalla legislazione vigente sia per le pubbliche amministrazioni sia per i privati, sono soddisfatti a tutti gli effetti, fatto salvo quanto indicato dall'art. 7, qualora il processo di conservazione venga effettuato con le modalità di cui agli articoli 3 e 4.
2. I documenti informatici, anche sottoscritti, così come individuati nell'art. 1, lettera f), possono essere archiviati elettronicamente prima di essere sottoposti al processo di conservazione. Per l'archiviazione elettronica non sussistono gli obblighi di cui alla presente deliberazione.

Art. 3.

Conservazione sostitutiva di documenti informatici

1. Il processo di conservazione sostitutiva di documenti informatici, anche sottoscritti, così come individuati nell'art. 1, lettera f), e, eventualmente, anche delle loro impronte, avviene mediante memorizzazione su supporti ottici e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo.
2. Il processo di riversamento sostitutivo di documenti informatici conservati avviene mediante memorizzazione su altro supporto ottico e termina con l'apposizione sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta il corretto svolgimento del processo. Qualora il processo riguardi documenti informatici sottoscritti, così come individuati nell'art. 1, lettera f), è inoltre richiesta l'apposizione del riferimento temporale e della firma digitale, da parte di un pubblico ufficiale, per attestare la conformità di quanto riversato al documento d'origine.

Art. 4.

Conservazione sostitutiva di documenti analogici

1. Il processo di conservazione sostitutiva di documenti analogici avviene mediante memorizzazione della relativa immagine direttamente sui supporti ottici, eventualmente, anche della relativa impronta, e termina con l'apposizione, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione che attesta così il
corretto svolgimento del processo.
2. Il processo di conservazione sostitutiva di documenti analogici originali unici si conclude con l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformità di quanto memorizzato al documento d'origine.
3. La distruzione di documenti analogici, di cui è obbligatoria la conservazione, è consentita soltanto dopo il completamento della procedura di conservazione sostitutiva, fatto salvo quanto previsto al comma 4 dell'art. 6 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
4. Il processo di riversamento sostitutivo di documenti analogici conservati avviene mediante memorizzazione su altro supporto ottico. Il responsabile ella conservazione, al termine del riversamento, ne attesta il corretto svolgimento con l'apposizione del riferimento temporale e della firma digitale sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi. Qualora il processo riguardi documenti originali unici di cui al comma 2, è richiesta l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformità di quanto riversato al documento d'origine.

Art. 5.

Responsabile della conservazione

1. Il responsabile del procedimento di conservazione sostitutiva:

a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;
b) archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
1) descrizione del contenuto dell'insieme dei documenti;
2) estremi identificativi del responsabile della conservazione;
3) estremi identificativi delle persone eventualmente delegate dal responsabile della conservazione, con l'indicazione dei compiti alle stesse assegnati;
4) indicazione delle copie di sicurezza;
c) mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
d) verifica la corretta funzionalità del sistema e dei programmi in gestione;
e) adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
f) richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
g) definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
h) verifica periodicamente, con cadenza non superiore a cinque
anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.
2. Il responsabile del procedimento di conservazione sostitutiva può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate.
3. Il procedimento di conservazione sostitutiva può essere affidato, in tutto o in parte, ad altri soggetti, pubblici o privati, i quali sono tenuti ad osservare quanto previsto dalla presente deliberazione.
4. Nelle amministrazioni pubbliche il ruolo di pubblico ufficiale è svolto dal dirigente dell'ufficio responsabile della conservazione dei documenti o da altri dallo stesso formalmente designati, fatta eccezione per quanto previsto dall'art. 3, comma 2, e dall'art. 4, commi 2 e 4, casi nei quali si richiede l'intervento di soggetto diverso della stessa amministrazione.

Art. 6.

Obbligo di esibizione

1. Il documento conservato deve essere reso leggibile in qualunque momento presso il sistema di conservazione sostitutiva e disponibile, a richiesta, su supporto cartaceo.
2. Il documento conservato può essere esibito anche per via telematica.
3. Qualora un documento conservato venga esibito su supporto cartaceo fuori dall'ambiente in cui è installato il sistema di conservazione sostitutiva, deve esserne dichiarata la conformità da parte di un pubblico ufficiale se si tratta di documenti per la cui conservazione è previsto il suo intervento.

Art. 7.

Procedure operative

1. A qualsiasi soggetto pubblico o privato che intenda avvalersi del processo di conservazione sostitutiva dei documenti è consentita l'adozione di accorgimenti e procedure integrative, nel rispetto di quanto stabilito nella presente deliberazione.
2. Le pubbliche amministrazioni comunicano preliminarmente al Centro nazionale per l'informatica nella pubblica amministrazione le procedure integrative che intendono adottare ai sensi del comma 1.

Art. 8.

Altri supporti di memorizzazione

1. Tenuto conto dell'evoluzione tecnologica e della disciplina dettata dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è data facoltà alle pubbliche amministrazioni e ai privati, ove non ostino particolari motivazioni, di utilizzare, nei processi di conservazione sostitutiva e di riversamento sostitutivo, un qualsiasi supporto di memorizzazione, anche non ottico, comunque idoneo a garantire la conformità dei documenti agli originali, nel rispetto delle modalità previste dalla presente deliberazione.

Art. 9.

Sistemi di conservazione preesistenti

1. Le regole tecniche dettate con le deliberazioni n. 15 del 28 luglio 1994, n. 24 del 30 luglio 1998 e n. 42 del 13 dicembre 2001 continuano ad applicarsi ai sistemi di conservazione sostitutiva già esistenti o in corso di acquisizione al momento della pubblicazione della presente deliberazione.

2. I documenti conservati in osservanza delle regole tecniche indicate al comma 1 possono essere riversati in un sistema di conservazione sostitutiva tenuto in conformità alle regole tecniche dettate con la presente deliberazione.

Roma, 19 febbraio 2004

Il presidente: Zoffoli

La prima legge regionale ad hoc in materia di procedure informatiche nella pubblica amministrazione è della Toscana.

NUMERO SCHEDA: 4432

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

NATURA ATTO: LEGGE REGIONALE

DATA ATTO: 26/01/2004

NUM. ATTO: 1

La legge regionale della Toscana "Promozione dell'amministrazione elettronica e della società dell'informazione e della conoscenza nel sistema regionale. Disciplina della "Rete telematica regionale toscana" costituisce la prima legge regionale *ad hoc* in materia di procedure informatiche nella pubblica amministrazione.

Attraverso la legge regionale 26 gennaio 2004, n. 1 la Toscana intende portare a regime il consenso istituzionale nella materia di riferimento, consolidando così l'esperienza della Rete telematica regionale toscana (derivata dal Piano di indirizzo approvato dal Consiglio regionale il 21 maggio 1997) e valorizzandola in funzione di finalità sempre più ampie e complesse, collegate allo sviluppo della società dell'informazione nel sistema regionale.

La finalità è di allargare i diritti di cittadinanza e partecipazione, rimuovendo e prevenendo ogni possibile causa di marginalizzazione o esclusione.

Si riporta di seguito il testo della legge regionale.

LEGGE REGIONALE 26 gennaio 2004, n. 1

Promozione dell'amministrazione elettronica e della società dell'informazione e della conoscenza

Capo I - DISPOSIZIONI GENERALI

Art. 01 - Finalità

1. La Regione con la presente legge:

a) favorisce il processo di innovazione organizzativa e tecnologica delle pubbliche amministrazioni del territorio regionale in un contesto organizzato di cooperazione istituzionale;

b) promuove lo sviluppo della società dell'informazione e della conoscenza in ambito regionale a fini di

progresso sociale e miglioramento della qualità della vita, favorendo la realizzazione personale e professionale nonché forme di cittadinanza attiva.
2. Nel perseguimento delle finalità di cui al comma 1, la Regione opera per rimuovere e prevenire gli ostacoli che di fatto impediscono la piena parità di accesso alle informazioni e alle tecnologie dell'informazione e della comunicazione, tenendo conto in particolare delle situazioni di disabilità, disagio economico e sociale e diversità culturale.

Art. 02 - Oggetto

1. La presente legge ha ad oggetto la programmazione e la promozione delle attività volte a:
a) realizzare modalità di amministrazione elettronica a fini sia di semplificazione, trasparenza e integrazione dei processi interni, sia di efficienza dei servizi per i cittadini e le imprese;
b)contribuire ad attuare una strategia organica ed unitaria per lo sviluppo della società dell'informazione e della conoscenza.
2. E' altresì oggetto della presente legge la disciplina della Rete Telematica Regionale Toscana (RTRT), di seguito denominata Rete, quale forma stabile di coordinamento del sistema regionale delle autonomie locali e di cooperazione del sistema stesso con altri soggetti, pubblici e privati, nelle materie di cui al comma 1, nei modi e con i procedimenti previsti al Capo II.

Art. 03 - Definizioni

1. Ai fini della presente legge si intende per:
a) amministrazione elettronica: l'organizzazione delle attività delle pubbliche amministrazioni fondata sull'impiego esteso e integrato delle tecnologie dell'informazione e della comunicazione nello svolgimento delle funzioni e nell'erogazione dei servizi;
b) società dell'informazione e della conoscenza: l'assetto delle società industriali avanzate, basato sulla centralità dell'informazione e della conoscenza quali risorse essenziali per lo sviluppo economico, sociale e culturale;
c) punti di accesso assistito: postazioni per l'accesso in via telematica a servizi pubblici, da utilizzare con l'assistenza di personale addetto;
d) programma a codice sorgente aperto: programma per elaboratore la cui licenza di distribuzione consente all'utente di accedere al codice sorgente per studiarne il funzionamento, apportarvi modifiche, mantenerlo nel tempo, estenderlo e ridistribuirlo;
e) interconnessione di reti: collegamento tra più reti, anche tecnicamente differenti, atto a costituire un sistema integrato in grado di trasferire informazioni e di erogare servizi;
f) interoperabilità dei sistemi: capacità di sistemi tecnicamente differenti di interagire e condividere dati e programmi informatici;
g) cooperazione applicativa: modalità operativa di procedure informatiche diverse che cooperano nello svolgimento di una stessa funzione o di funzioni diverse tra loro correlate;
h) reti civiche unitarie: aggregazioni di soggetti costituite su base territoriale per la promozione e lo sviluppo dell'amministrazione elettronica e della società dell'informazione nel territorio di riferimento.

Art. 04 - Principi e criteri guida

1. Nel perseguimento delle finalità di cui all'articolo 1, comma 1, lettera a), la Regione e i soggetti di cui all'articolo 8, comma 2, operano conformandosi ai seguenti principi e criteri guida:
a) sviluppo coordinato dei sistemi informativi pubblici, valorizzazione e condivisione del patrimonio informativo pubblico, entrambi da perseguire secondo i modelli di cooperazione istituzionale definiti nella presente legge;
b) valorizzazione, ai fini della presente legge, delle aggregazioni di soggetti costituite su base tematica o territoriale, comprese le reti civiche unitarie, e dei raccordi con le articolazioni territoriali dell'amministrazione statale;
c) utilizzazione di standard informativi e documentali aperti negli scambi tra amministrazioni pubbliche e con riferimento ai dati da rendere pubblici;
d) rispetto della normativa in materia di tutela delle persone e degli altri soggetti riguardo al trattamento dei dati personali, nonché in materia di legittima titolarità dei dati;
e) qualità dei dati in termini di correttezza, aggiornamento, completezza e coerenza, nonché di integrità degli stessi nella gestione telematica, anche mediante l'adozione di tecniche di marchiatura elettronica e criptazione;
f) salvaguardia della sicurezza dei dati, dei sistemi, delle reti e dei servizi mediante l'adozione di misure

tecniche e organizzative adeguate;
g) diffusione di strumenti di identificazione elettronica e di procedure di accesso ai servizi telematici;
h) diffusione di procedure telematiche di acquisto per l'approvvigionamento di beni e servizi da parte delle pubbliche amministrazioni, nel rispetto delle specificità e dello sviluppo dei mercati locali;
i) promozione, sostegno ed utilizzo preferenziale di soluzioni basate su programmi con codice sorgente aperto, in osservanza del principio di neutralità tecnologica, al fine di abilitare l'interoperabilità di componenti prodotti da una pluralità di fornitori, di favorirne la possibilità di riuso, di ottimizzare le risorse e di garantire la piena conoscenza del processo di trattamento dei dati.
2. Nel perseguimento delle finalità di cui all'articolo 1, comma 1, lettera b), la Regione e i soggetti di cui all'articolo 8, comma 2, operano conformandosi ai seguenti principi e criteri guida:
a) valorizzazione dei soggetti istituzionali, economici e sociali come produttori d'informazioni e di contenuti condivisi in rete;
b) educazione all'uso consapevole del patrimonio informativo e statistico delle pubbliche amministrazioni;
c) educazione all'uso consapevole della Rete e degli strumenti con particolare riferimento ai vantaggi connessi all'utilizzo di programmi liberi e a codice sorgente aperto;
d) adozione di misure, soluzioni tecnologiche, standard e pratiche di sviluppo che favoriscano l'inclusione sociale, garantendo l'accessibilità, con specifica attenzione alle diverse abilità e promuovendo l'usabilità dei sistemi informativi;
e) incentivazione, qualificazione e coordinamento dei servizi di rete per uno sviluppo socio-economico equilibrato del territorio regionale, anche attraverso la costituzione di punti di accesso assistito;
f) sostegno alle famiglie, alle scuole e ad altre formazioni sociali nell'acquisizione di concrete possibilità di accesso ai servizi erogati con strumenti tecnologici e telematici;
g) realizzazione di iniziative e adozione di misure rivolte a generare la fiducia degli utenti nei diversi usi della rete;
h) utilizzo delle tecnologie dell'informazione e della comunicazione con modalità adeguate a stimolare lo sviluppo economico del territorio in termini di competenza, di qualificazione delle opportunità professionali, di innovazione e di avanzamento della conoscenza;
i) stimolo alle imprese che operano nel settore delle tecnologie dell'informazione e della comunicazione per lo sviluppo di servizi di qualità attraverso procedure di accreditamento nonché di qualificazione e organizzazione della domanda;
l) valorizzazione del complesso delle conoscenze e dei risultati scientifici, al fine di promuovere il trasferimento culturale e tecnologico e l'innovazione sociale e produttiva.

Art. 05 - Trattamento di dati personali

1. La realizzazione di sistemi e servizi informativi pubblici per la promozione e lo sviluppo della società dell'informazione e della conoscenza costituisce svolgimento di funzioni istituzionali ai fini del trattamento di dati personali da parte della Regione e degli altri enti del sistema regionale delle autonomie locali.

Art. 06 - Coordinamento delle politiche e delle attività di settore

1. Al fine di garantire il perseguimento coerente degli obiettivi di cui all'articolo 1, la Regione coordina i propri interventi con quelli dello Stato e delle altre regioni mediante la partecipazione ad appositi organismi nazionali, prioritariamente nell'ambito del sistema delle Conferenze previsto dal decreto legislativo 28 agosto 1997, n. 281 (Definizione ed ampliamento delle attribuzioni della Conferenza permanente per i rapporti tra lo Stato, le regioni e le Province autonome di Trento e Bolzano ed unificazione, per le materie ed i compiti di interesse comune delle regioni, delle province e dei comuni, con la Conferenza Stato-città ed autonomie locali), nonché attraverso strumenti negoziali di attuazione delle politiche di settore.
2. Al fine di assicurare l'esercizio unitario da parte della Regione e dei soggetti di cui all'articolo 8, comma 2, delle funzioni e delle attività collegate alla gestione del patrimonio informativo, all'attuazione dell'amministrazione elettronica e alla promozione della società dell'informazione e della conoscenza nel sistema regionale, la Regione, nel rispetto delle disposizioni emanate dallo Stato ai sensi dell'articolo 117, comma 2, lettera r), della Costituzione, definisce, sulla base di determinazioni assunte dalla Rete, le misure di carattere tecnico a valenza generale alle quali i soggetti di cui all'articolo 8, comma 2, sono tenuti a conformarsi.

Art. 07 - Programmazione regionale e locale

1. Nell'ambito delle politiche definite dal programma regionale di sviluppo e secondo la normativa regionale in materia di programmazione, la Regione adotta il Programma regionale per la promozione e lo sviluppo dell'amministrazione elettronica e della società dell'informazione e della conoscenza nel sistema regionale, di seguito denominato Programma, nei modi previsti dalla presente legge.

2. Il Programma, di durata triennale, è approvato dal Consiglio regionale su proposta della Giunta regionale, formulata tenendo conto degli indirizzi e dei documenti programmatici della Rete. Tale Programma contiene:

a) gli interventi a sostegno degli obiettivi di cui all'articolo 1, comma 1, lettera a) e lettera b);

b) gli interventi a sostegno della formazione del personale della Regione e degli enti locali, da perseguire preferibilmente in forma stabile;

c) gli interventi a sostegno della gestione e dello sviluppo dell'infrastruttura tecnologica, nonché dei servizi e delle attività della Rete.

3. Il Programma è attuato annualmente attraverso il Piano di attività annuale della Rete di cui all'articolo 17. Per la parte di propria competenza la Giunta regionale approva detto Piano mediante deliberazione che viene comunicata al Consiglio regionale e al Consiglio delle autonomie locali.

4. Per le finalità di cui all'articolo 1 e nel rispetto dei rispettivi ambiti di autonomia gli enti locali coordinano i propri interventi con quelli definiti nella programmazione regionale attraverso la partecipazione alle attività e ai progetti della Rete, nonché attraverso eventuali strumenti negoziali di attuazione.

5. I finanziamenti regionali degli interventi degli enti locali sono graduati, sulla base di criteri condivisi nella Rete, in relazione sia alla congruenza degli interventi stessi con gli atti di programmazione di cui al presente articolo, sia al loro livello di integrazione territoriale e di compartecipazione al finanziamento.

CapoII - DISCIPLINA DELLA RETE TELEMATICA REGIONALE TOSCANA

Art. 08 - Soggetti della Rete

1. Il presente capo individua e disciplina i soggetti e i procedimenti con i quali si realizza la Rete come definita all'articolo 2, comma 2.

2. Fanno parte della Rete la Regione, gli enti e le agenzie regionali, gli enti e le aziende sanitarie pubbliche e, mediante le convenzioni di cui all'articolo 10, i comuni singoli o associati, le province, i circondari istituiti ai sensi della legislazione regionale vigente, la città metropolitana, le comunità montane.

3. Fanno altresì parte della Rete, mediante le convenzioni di cui all'articolo 10, le università e gli istituti ed enti di ricerca, le amministrazioni periferiche dello Stato, i soggetti del Servizio socio-sanitario regionale, le aziende di servizi pubblici locali, le camere di commercio e le altre autonomie funzionali, nonché le categorie economiche, le libere professioni e le altre associazioni.

Art. 09 - Compiti della Regione nella Rete

1. La Regione ha compiti di promozione, cofinanziamento e gestione dell'infrastruttura tecnologica della Rete, ivi compresi i servizi di base e per la cooperazione applicativa. La Regione inoltre, tramite i propri uffici, fornisce ogni altro servizio funzionale allo svolgimento delle attività e al perseguimento degli obiettivi della Rete determinati dal Comitato strategico.

Art. 10 - Convenzioni di adesione alla Rete

1. Le convenzioni di adesione alla Rete sono predisposte dal Comitato strategico di cui all'articolo 13 e sottoscritte dai soggetti di cui all'articolo 8 e dal Presidente della Giunta regionale o suo delegato.

2. Con la convenzione di cui al comma 1 i soggetti di cui all'articolo 8, comma 2, si impegnano a:

a) adempiere gli obblighi ed oneri informativi stabiliti con leggi o regolamenti dello Stato o della regione secondo le modalità di cui all'articolo 18;

b) fornire l'accesso gratuito ai propri servizi telematici da parte delle pubbliche amministrazioni del territorio regionale;

c) contribuire con il proprio patrimonio informativo ai processi di e-government nell'interesse e perseguimento degli obiettivi della Rete;

d) realizzare servizi di comunicazione integrati, finalizzati ad aumentare il livello di comunicazione e cooperazione sia tra i soggetti della Rete, sia con altri soggetti esterni;

e) comunicare al Comitato strategico di cui all'articolo 13 le informazioni necessarie per l'istituzione e l'aggiornamento dei servizi centrali di gestione dell'infrastruttura;

f) compartecipare al finanziamento delle attività della Rete nelle forme determinate dalla Rete stessa, salvo

il rispetto dell'autonomia di bilancio dei singoli enti;
g) attuare i piani di attività e le decisioni della Rete secondo le norme dei rispettivi ordinamenti;
h) riconoscere al Coordinatore della Rete la funzione di cui all'articolo 14, comma 1.

Art. 11 - Forme organizzative della Rete

1. La Rete opera attraverso le seguenti forme regolate:
a) l'Assemblea;
b) il Comitato strategico;
c) il Coordinatore della Rete;
d) la Direzione tecnico-operativa;
e) l'Osservatorio degli utenti.

Art. 12 - Assemblea

1. L'Assemblea è composta dai rappresentanti dei soggetti aderenti e svolge funzioni di indirizzo generale e proposta in relazione alle attività e ai progetti della Rete.
2. L'Assemblea disciplina la propria organizzazione con atto approvato dalla maggioranza assoluta dei componenti.
3. L'Assemblea, nella sua componente di cui all'articolo 8, comma 2, disciplina, inoltre, la composizione del Comitato strategico.

Art. 13 - Comitato strategico

1. Il Comitato strategico svolge funzioni d'indirizzo e di direzione delle attività della Rete. Il Comitato promuove le prassi evolutive della Rete e concorda con i soggetti di cui all'articolo 8, comma 3, le modalità della loro partecipazione, anche al fine della definizione delle convenzioni di cui all'articolo 10.
2. Il Comitato, presieduto dal Presidente della Giunta regionale o suo delegato, è composto da non più di trenta rappresentanti dei soggetti di cui all'articolo 8, comma 2; fanno altresì parte del Comitato un rappresentante del Consiglio delle autonomie locali e un rappresentante di ciascuna delle associazioni degli enti locali.
3.Il Comitato disciplina il proprio funzionamento e le modalità organizzative con atti approvati dalla maggioranza assoluta dei componenti.

Art. 14 - Coordinatore della Rete

1. Il Coordinatore cura i rapporti della Rete coi soggetti pubblici e privati nei limiti delle decisioni assunte nell'ambito della Rete stessa e coordina l'insieme delle risorse tecniche e organizzative attivate.
2. Il Comitato strategico disciplina le funzioni e le modalità di nomina del Coordinatore della Rete.
3. Ove richiesto dalle competenti commissioni del Consiglio regionale, il Coordinatore è tenuto a fornire ogni informazione relativa alle attività e al funzionamento della Rete.

Art. 15 - Direzione tecnico-operativa

1. La Direzione tecnico-operativa svolge funzioni istruttorie e quelle assegnate per la definizione di standards nell'ambito della Rete, per la sua interconnessione con altre reti, per l'interoperabilità dei sistemi e la cooperazione applicativa.
2. La Direzione predispone il Piano di attività di cui all'articolo 17 al fine della sua adozione e redige il Documento di monitoraggio annuale delle attività della Rete, in vista della approvazione del Piano stesso.
3. Il Comitato strategico disciplina le funzioni, la composizione, le modalità di nomina e di organizzazione della Direzione tecnico-operativa.

Art. 16 - Osservatorio degli utenti

1. Al fine di favorire l'efficacia dei servizi telematici delle pubbliche amministrazioni del territorio regionale, è istituito l'Osservatorio degli utenti presso la Direzione tecnico operativa.
2. Il Comitato strategico disciplina la composizione e le modalità di organizzazione dell'Osservatorio, assicurandone il coordinato rapporto con le altre forme organizzative della Rete e garantendo la partecipazione in esso delle varie componenti di carattere economico e sociale della società civile organizzata, prevedendo modalità di informazione al Consiglio regionale dei risultati delle attività dell'Osservatorio stesso.

Art. 17 - Piano di attività annuale della Rete

1. Il Piano di attività annuale della Rete:
a) definisce le attività di gestione e sviluppo della Rete con riguardo alle infrastrutture, ai servizi e ai contenuti, previa verifica dei risultati conseguiti nell'ambito della Rete stessa;
b) indica gli obiettivi e le azioni di impulso e sostegno per l'attuazione dell'amministrazione elettronica e la

promozione della società dell'informazione e della conoscenza;
c) recepisce e raccorda le linee dei progetti concordati e cofinanziati dai soggetti della Rete.
2. Il Piano è adottato dal Comitato strategico ed è successivamente trasmesso, insieme al Documento di monitoraggio di cui all'articolo 15, comma 2, alla Giunta regionale che lo approva secondo la procedura di cui all'articolo 7, comma 3.
Art. 18 - Adempimento di obblighi ed oneri informativi
1. Ai fini dello scambio delle informazioni relative alle funzioni di propria competenza, la Regione, gli enti e le agenzie regionali, gli enti e le aziende sanitarie pubbliche, adempiono in forma elettronica gli obblighi e gli oneri informativi stabiliti con leggi o regolamenti dello Stato o della regione, avvalendosi della Rete e con le modalità operative adottate nell'ambito della stessa ove non diversamente disposto.
Art. 19 - Norma finanziaria
1. Agli oneri derivanti dall'applicazione della presente legge si provvede con imputazione alle Unità revisionali di base (UPB) "Innovazione tecnologica, organizzativa e sviluppo risorse umane per l'attuazione delle politiche regionali" n. 146 e n. 141 del bilancio di previsione 2004. Per i successivi esercizi si provvederà con le relative leggi di bilancio.
Capo III - DISPOSIZIONI TRANSITORIE
Art. 20 - Norme transitorie
1. Gli organismi della Rete già costituita con deliberazione del Consiglio regionale 21 maggio 1997, n. 172 (Piano di indirizzo per l'attuazione della Rete telematica regionale) operanti alla data di entrata in vigore della presente legge continuano a svolgere le funzioni fino alla convocazione della prima Assemblea e alla creazione degli organismi corrispondenti istituiti con la presente legge.
2. Sono fatti salvi gli atti di adesione alla Rete sottoscritti prima dell'entrata in vigore della presente legge fino alla sottoscrizione delle convenzioni di cui all'articolo 10.
3. La prima Assemblea è convocata dal Presidente della Giunta regionale entro tre mesi dalla data di entrata in vigore della presente legge.
Art. 21 - Entrata in vigore
1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione.

Pubblicata sulla G.U. la direttiva che fornisce indicazioni sulla possibilità di acquisizione ed utilizzo di programmi informatici "open source" da parte delle pubbliche amministrazioni.

NUMERO SCHEDA: 4386

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: GAZZETTA UFFICIALE

NUMERO: 31

DATA: 07/02/1004

NATURA ATTO: DIRETTIVA

DATA ATTO: 19/12/2003

NUM. ATTO: 2003

ORGANO: MINISTERI

E' stata pubblicata sulla G.U. del 7 febbraio 2004 la direttiva del Ministro per l'Innovazione e le Tecnologie 19 dicembre 2003 “Sviluppo ed utilizzazione dei programmi informatici da parte delle pubbliche amministrazioni" che fornisce indicazioni sulla possibilità di acquisizione ed utilizzo di programmi informatici "*open source*".
Tra le possibili soluzioni tecnologiche utilizzabili dalle P.A. esistono anche quelle "open source", ovvero applicazioni il cui codice sorgente può essere liberamente studiato, copiato, modificato e ridistribuito.
Le P. A., nella scelta delle soluzioni informatiche disponibili sul mercato, dovranno seguire criteri dettati dalle loro specifiche esigenze ma anche da altri elementi quali:

- la trasferibilità ad altre Amministrazioni delle soluzioni acquisite;
- l'interoperabilità e la cooperazione applicativa tra le amministrazioni;
- la non dipendenza da un unico fornitore o da un'unica tecnologia proprietaria;
- la disponibilità del codice sorgente per ispezione e tracciabilità;
- l' esportabilità di dati.

Le Amministrazioni dovranno poter "acquisire la proprietà" dei programmi informatici sviluppati per loro dalle imprese fornitrici attraverso idonee clausole contrattuali, e poter "trasferire la titolarità delle licenze d'uso" ad altre amministrazioni senza oneri aggiuntivi. Dovrà infine essere prevista, ove possibile, in apposite clausole la possibilità di "consentire il riuso" dei programmi sviluppati anche su altre piattaforme.

Si riporta di seguito il testo della direttiva.

PRESIDENZA DEL CONSIGLIO DEI MINISTRI - DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE - DIRETTIVA 19 dicembre 2003 (in G.U. n. 31 del 7 febbraio 2004) - Sviluppo ed utilizzazione dei programmi informatici da parte delle pubbliche amministrazioni.

1. Finalità.

Con la presente direttiva si forniscono alle pubbliche amministrazioni indicazioni e criteri tecnici e operativi per gestire più efficacemente il processo di predisposizione o di acquisizione di programmi informatici. In particolare, nella presente direttiva si indica come le pubbliche amministrazioni debbano tener conto della offerta sul mercato di una nuova modalità di sviluppo e diffusione di programmi informatici, definita «open source» o «a codice sorgente aperto». L'inclusione di tale nuova tipologia d'offerta all'interno delle soluzioni tecniche tra cui scegliere, contribuisce ad ampliare la gamma delle opportunità e delle possibili soluzioni, in un quadro di equilibrio, di pluralismo e di aperta competizione.

2. Definizioni.

Ai fini della presente direttiva si intende:

a) per «formato dei dati» la modalità con cui i dati vengono rappresentati elettronicamente in modo che i programmi informatici possano elaborarli. Il formato specifica la corrispondenza fra la rappresentazione binaria e i dati rappresentati (testo, immagini statiche o dinamiche, suono, ecc.).
Esempi di formati sono Bitmap, GIF, JPEG, ecc.;

b) per «formato aperto», un formato dei dati reso pubblico e documentato esaustivamente;

c) per «tecnologia proprietaria», una tecnologia posseduta in esclusiva da un soggetto che in genere ne mantiene segreto il funzionamento;

d) per «formato proprietario» un formato di dati utilizzato in esclusiva da un soggetto che potrebbe modificarlo a proprio piacimento;

e) per «standard» una specifica o norma condivisa da una comunità. Lo standard può essere emanato da un ente di standardizzazione oppure essersi imposto di fatto (industry standard). Nel caso dei formati dei dati

o dei documenti, un formato è standard quando è definito da un ente di standardizzazione (per esempio, il formato XML), o è di fatto condiviso da una comunità (per esempio, il formato PDF);
f) per «interoperabilita» la capacità di sistemi informativi anche eterogenei di condividere, scambiare e utilizzare gli stessi dati e funzioni d'interfaccia;
g) per «programmi informatici ad hoc o custom» applicazioni informatiche sviluppate o mantenute da un fornitore per soddisfare specifiche esigenze di uno o più clienti. Normalmente questo tipo di sviluppo viene eseguito all'interno di un contratto di servizio per il quale il cliente corrisponde al fornitore un compenso;
h) per «programmi a licenza d'uso», o «pacchetti», applicazioni informatiche che vengono cedute in uso (e non in proprieta) dal fornitore al cliente. Tale cessione d'uso è regolata da opportune licenze che indicano i vincoli e i diritti che sono garantiti al titolare della licenza stessa;
i) per «programmi di tipo proprietario», applicazioni informatiche basate su tecnologia di tipo proprietario, cedute in uso dietro pagamento di una licenza, che garantisce solo la fornitura del codice eseguibile e non del codice sorgente. Esempi di tali prodotti sono MS Windows, IBM DB2, Oracle DB;
j) per «programmi a codice sorgente aperto» o «open source», applicazioni informatiche il cui codice sorgente può essere liberamente studiato, copiato, modificato e ridistribuito;
k) per «costo totale di possesso», l'insieme dei costi che nel corso dell'intera vita operativa di un sistema informativo è necessario sostenere affinchè esso sia utilizzabile proficuamente dall'utenza;
l) per «costo di uscita», l'insieme dei costi da sostenere per abbandonare una tecnologia o migrare verso una tecnologia o soluzione informatica differente. Comprende i costi di conversione dati, di aggiornamento dell'hardware, di realizzazione interfaccia e di formazione;
m) per «piattaforma», infrastruttura informatica, comprendente sia hardware che software, su cui vengono elaborati i programmi applicativi;
n) per «portabilita», possibilità di trasferire un programma informatico da una piattaforma a un'altra.

3. Analisi comparativa delle soluzioni.

1. Le pubbliche amministrazioni, nel rispetto della legge 7 agosto 1990, n. 241 e del decreto legislativo 12 febbraio 1993, n. 39, acquisiscono programmi informatici a seguito di una valutazione comparativa tra le diverse soluzioni disponibili sul mercato.
2. In particolare, valutano la rispondenza alle proprie esigenze di ciascuna delle seguenti soluzioni tecniche:
a) sviluppo di programmi informatici ad hoc, sulla scorta dei requisiti indicati dalla stessa amministrazione committente;
b) riuso di programmi informatici sviluppati ad hoc per altre amministrazioni;
c) acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso;
d) acquisizione di programmi informatici a codice sorgente aperto;
e) acquisizione mediante combinazione delle modalità di cui alle lettere precedenti.
3. Le pubbliche amministrazioni valutano quale soluzione, tra le disponibili, risulta più adeguata alle proprie esigenze mediante comparazioni di tipo tecnico ed economico, tenendo conto anche del costo totale di possesso delle singole soluzioni e del costo di uscita. In sede di scelta della migliore soluzione si tiene altresì conto del potenziale interesse di altre amministrazioni al riuso dei programmi informatici, dalla valorizzazione delle competenze tecniche acquisite, della più agevole interoperabilità. La prospettazione degli elementi di cui sopra è peraltro oggetto di valutazione da parte del Centro nazionale per l'informatica nella pubblica amministrazione in sede di rilascio del parere di cui all'art. 8 del decreto legislativo 12 febbraio 1993, n. 39. La suindicata valutazione va inclusa nell'ambito dello studio di fattibilità prescritto dall'art. 13 del decreto legislativo 12 febbraio 1993, n. 39, allorchè si tratti di contratti di grande rilievo.

4. Criteri tecnici di comparazione.

Le pubbliche amministrazioni, nella predisposizione o nell'acquisizione dei programmi informatici, privilegiano le soluzioni che presentino le seguenti caratteristiche:
a) soluzioni informatiche che, basandosi su formati dei dati e interfacce aperte e standard, assicurino 1'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione, salvo che ricorrano peculiari ed eccezionali esigenze di sicurezza e segreto;
b) soluzioni informatiche che, in assenza di specifiche ragioni contrarie, rendano i sistemi informatici non dipendenti da un unico fornitore o da un'unica tecnologia proprietaria; la dipendenza è valutata tenendo conto dell'intera soluzione;
c) soluzioni informatiche che, con il preventivo assenso del C.N.I.P.A. ed in assenza di specifiche ragioni contrarie, garantiscano la disponibilità del codice sorgente per ispezione e tracciabilità da parte delle

pubbliche amministrazioni, ferma la non modificabilità del codice, fatti salvi i diritti di proprietà intellettuale del fornitore e fermo l'obbligo dell'amministrazione di garantire segretezza o riservatezza;
d) programmi informatici che esportino dati e documenti in più formati, di cui almeno uno di tipo aperto.
5. Proprietà dei programmi software.
Nel caso di programmi informatici sviluppati ad hoc, l'amministrazione committente acquisisce la proprietà del prodotto finito, avendo contribuito con proprie risorse all'identificazione dei requisiti, all'analisi funzionale, al controllo e al collaudo del software realizzato dall'impresa contraente. Sarà cura dei committenti inserire, nei relativi contratti, clausole idonee ad attestare la proprietà dei programmi.
6. Trasferimento della titolarità delle licenze d'uso.
Le pubbliche amministrazioni si assicurano contrattualmente la possibilità di trasferire la titolarità delle licenze d'uso dei programmi informatici acquisiti, nelle ipotesi in cui all'amministrazione che ha acquistato la licenza medesima ne subentri un'altra nell'esercizio delle stesse attività; parimenti va contrattualmente previsto l'obbligo del fornitore di trasferire, su richiesta dell'amministrazione, senza oneri ulteriori per l'amministrazione stessa, e salve eccezionali cause ostative, la licenza d'uso al gestore subentrante, nel caso in cui l'amministrazione trasferisca a terzi la gestione di proprie attività, ovvero l'obbligo di emettere, laddove possibile, nuova licenza d'uso con i medesimi effetti nei confronti del nuovo gestore.
7. Riuso.
1. Al fine di favorire il riuso dei programmi informatici di proprietà delle amministrazioni, nei capitolati o nelle specifiche di progetto dovrà essere previsto, ove possibile, che i programmi sviluppati ad hoc siano facilmente portabili su altre piattaforme.
2. Nei contratti di acquisizione di programmi informatici sviluppati per conto e a spese delle amministrazioni, le stesse includono clausole, concordate con il fornitore e che tengano conto delle caratteristiche economiche ed organizzative di quest'ultimo, volte a vincolarlo, per un determinato lasso di tempo, a fornire, su richiesta di altre amministrazioni, servizi che consentono il riuso delle applicazioni. Le clausole suddette definiscono le condizioni da osservare per la prestazione dei servizi indicati.
8. Supporto alle amministrazioni.
Il Centro nazionale per l'informatica nella pubblica amministrazione promuove l'attuazione della presente direttiva e fornisce alle amministrazioni adeguato supporto.

I risultati di una ricerca del Censis evidenziano che in testa alla graduatoria dell'innovazione tecnologica ci sono le piccole Regioni.

NUMERO SCHEDA: 3675

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

NATURA ATTO: RICERCA

DATA ATTO: 18/08/2003

I risultati di una ricerca condotta dal Censis per «Il Sole-24 Ore del lunedì» sulle aree digitali evidenzia che sono le piccole Regioni a dimostrare di avere assimilato meglio la nuova filosofia: Trentino-Alto Adige e Basilicata sono rispettivamente al primo e secondo posto per quanto riguarda l'uso domestico del pc e per il numero di persone che navigano nel web.
La ricerca Censis consegna l'immagine di un'Italia molto variegata, dove comunque, la qualità del sistema imprenditoriale e delle infrastrutture fa la differenza. La Lombardia,

per tradizione all'avanguardia dal punto di vista tecnologico, mantiene la testa della graduatoria generale, realizzata calibrando fra loro le diverse categorie sotto esame. Alle spalle della Lombardia emergono Veneto, Toscana e Sicilia (per gli investimenti It) e Calabria e Abruzzo (per la nascita di nuove imprese).
Il risultato della ricerca evidenzia un modello di sviluppo regionale che ha messo al centro il cambiamento e l'innovazione e dimostra che le regioni hanno una grande potenzialità per aggregare la domanda di sviluppo tecnologico, darle forma e veicolarla a tutte le istituzioni competenti.
Tra le aree di maggiore sviluppo conferma la sua attenzione all'It l'Emilia Romagna, quarta nella graduatoria globale e prima nella categoria «Città digitali».
Oltre alle iniziative delle singole regioni, sono anche le attività di concertazione e sinergia che rendono l'innovazione tecnologica più efficace sul territorio. E' attivo un coordinamento nazionale dei «Centri regionali di competenza» per l'e-government e la società dell'informazione. I Centri formano un network di risorse che opera sul territorio regionale e appoggia le amministrazioni locali nella diffusione delle nuove tecnologie. Il progetto, nato da un accordo tra il ministro per l'Innovazione e le Tecnologie e le Regioni, ha favorito gli scambi e le azioni comuni su scala interregionale

In Gazzetta Ufficiale il decreto sui progetti strategici per il settore informatico.

NUMERO SCHEDA: 3373

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: MINISTERI

RIFERIMENTO NORMATIVO: l. 3/2003

NATURA ATTO: DECRETO

DATA ATTO: 14/05/2003

ORGANO: MINISTERI

Sulla Gazzetta Ufficiale è stato pubblicato il decreto 14 maggio 2003 (emanato in attuazione della legge 3/2003, per la quale si segnalano le schede nn. 2262 e 2371) dal dipartimento per l'Innovazione tecnologica sull'utilizzo e la disciplina delle funzioni relative al Fondo di finanziamento per i progetti strategici nel settore informatico.
Il provvedimento consta disposizioni sia sull'utilizzo dei fondo di finanziamento che sulla gestione ed il monitoraggio dei progetti.

Si allega il testo.

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE

DECRETO 28 maggio 2004

UTILIZZO DEL FONDO DI FINANZIAMENTO PER I PROGETTI STRATEGICI NEL SETTORE INFORMATICO.

Art. 1.

Utilizzo del «Fondo di finanziamento per i progetti strategici nel settore informatico»

1. Ai sensi dell'art. 27, commi 1 e 2, primo periodo, della legge 16 gennaio 2003, n. 3, valutate le indicazioni espresse dal Comitato dei Ministri per la Società dell'Informazione nella seduta del 16 marzo 2004, sono individuati nell'allegato A del presente decreto grandi progetti di contenuto innovativo, di rilevanza strategica e di preminente interesse nazionale per lo sviluppo dei sistemi informativi e della società dell'informazione da sostenere con un finanziamento a valere sulle disponibilità del Fondo di cui al citato comma 2, da realizzarsi da parte dei soggetti proponenti con le modalità di cui al presente decreto.
2. Al finanziamento dei progetti individuati, di costo complessivamente pari a 247.000.000 di euro, si provvede quanto a 74.000.000 di euro con i fondi di pertinenza delle amministrazioni proponenti, quanto a 173.000.000 di euro a valere sulla disponibilità del Fondo di cui all'art. 27, commi 2, secondo periodo, e 4 della legge 16 gennaio 2003, n. 3, ripartiti nella misura di 25.138.000 euro quale rimanenza delle precedenti annualità, di 51.500.000 euro a valere sul 2004, di 65.000.000 di euro per il 2005 e di 31.362.000 euro per il 2006.
3. Nell'ambito della definizione progettuale e nel rispetto degli studi di fattibilità risultanti dall'attività istruttoria condotta dalla Segreteria tecnica del Comitato dei Ministri per la Società dell'Informazione, le amministrazioni proponenti sono autorizzate ad assumere impegni di spesa nei limiti dell'intera somma del finanziamento anche secondo quanto previsto dal comma 2 dell'art. 11-quater della legge 5 agosto 1978, n. 468. In caso di inadempienze, le risorse disponibili possono essere riprogrammate, sentito il Comitato dei Ministri per la Società dell'Informazione.
4. Ai sensi dell'art. 27, comma 5, della legge 16 gennaio 2003, n. 3, su proposta del Ministro per l'innovazione e le tecnologie formulata entro quindici giorni dalla data di pubblicazione del presente decreto, il Ministro dell'economia e delle finanze apporta con propri decreti le variazioni di bilancio occorrenti ad assicurare alle amministrazioni proponenti le somme necessarie al cofinanziamento del progetto.

Art. 2.

Gestione e monitoraggio dei progetti, attività di comunicazione

1. Il monitoraggio dell'attuazione di ciascun progetto é assicurato da ciascuna amministrazione proponente. Qualora un progetto interessi più amministrazioni, l'amministrazione proponente costituisce un Comitato di coordinamento, presieduto da un proprio rappresentante e composto da un rappresentante di ciascuna delle amministrazioni cointeressate. Entro trenta giorni dalla pubblicazione del presente decreto le amministrazioni interessate in ciascun progetto, così come individuate in allegato A, designano il proprio rappresentante all'interno dei Comitati di coordinamento.
2. Il Dipartimento per l'innovazione e le tecnologie verifica la coerenza dell'attuazione dei progetti di cui al presente decreto con gli indirizzi strategici del Ministro per l'innovazione e le tecnologie e con le decisioni assunte dal Comitato dei Ministri per la Società dell'Informazione.
3. Il Dipartimento per l'innovazione e le tecnologie assicura le iniziative di comunicazione, d'intesa con le amministrazioni interessate.

Il presente decreto sarà trasmesso agli organi di controllo per la registrazione e sarà pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

Rapporto conclusivo della Commissione ministeriale d'indagine sull'utilizzo di software nella P.A.

NUMERO SCHEDA: 3215

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

DATA: 17/06/2003

NATURA ATTO: RAPPORTO

DATA ATTO: 17/06/2003

ORGANO: MINISTERI

La Commissione ministeriale d'indagine sull'utilizzo di software nella P.A.- che ha operato in un arco temporale di cinque mesi, coinvolgendo nei lavori di studio numerosi e qualificati esperti della Pubblica Amministrazione, del mondo accademico e dell'industria - ha elaborato un rapporto conclusivo nel quale emerge che nel 2001 la Pubblica Amministrazione, centrale e locale, ha speso per l'acquisto di software 675 milioni di euro. Nell'ambito di tale cifra il 61% si è concentrato sullo sviluppo, manutenzione e gestione dei programmi custom - ossia sviluppati su commessa per una specifica Amministrazione- ; il restante 39% è stato impiegato per acquistare licenze di pacchetti software.
Dai dati contenuti nella relazione emerge che, malgrado l'evoluzione tecnologica e qualitativa di tali soluzioni ne renderebbe interessante l'utilizzo diffuso, i progetti di dimensioni significative restano comunque rari.
Il Rapporto conclusivo rappresenta una prima analisi dei seguenti aspetti:
- contesto internazionale;
- possibili criteri di valutazione per l'impiego del software OS nella PA;
- eventuali interventi sul piano della normazione e sul piano organizzativo.

In considerazione del fatto che il settore dell'ICT è caratterizzato da continue evoluzioni e da inattesi cambi di scenario, continuerà il monitoraggio del fenomeno software OS.

Il citato rapporto è consultabile sul sito web del Governo al seguente indirizzo:
http://www.governo.it/GovernoInforma/Dossier/open_source/open%20software%20PA.pdf

Firmato il decreto di regolamentazione dei servizi wi-fi ad uso pubblico (accesso ad internet senza fili).

NUMERO SCHEDA: 3113

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: MINISTERI

DATA: 03/05/2003

NATURA ATTO: REGOLAMENTO

DATA ATTO: 28/05/2003

ORGANO: MINISTERI

Il ministro delle Comunicazioni in data 28 maggio 2003 ha firmato il decreto che regolamenta l'uso del wi-fi, ovvero la possibilità di navigare in internet senza fili attraverso il computer portatile. Il provvedimento introduce in Italia la regolamentazione dei sistemi wi-fi ad uso pubblico, in locali aperti al pubblico o in aree confinate a frequentazione pubblica (ad es. gli aeroporti) : offre, cioè, la possibilità di installare reti di tipo Radio Lan per fornire al pubblico l'accesso ai servizi di comunicazione elettronica sulle bande di frequenza dei 2,4 e dei 5 GHz, mediante una semplice autorizzazione.
Il decreto prevede anche il rispetto delle norme sulla sicurezza ed integrità delle reti e stabilisce che la competenza a vigilare e, se ,anzionare eventuali illeciti spetta sia al Ministero che all'Autorita' Garante per le Comunicazioni, la quale a sua volta regolamentera' nel dettaglio per la tutela degli utenti e per il corretto funzionamento dei sistemi.

Si allega il testo del decreto.

Art. 1
(Definizioni)

1. Ai fini del presente decreto si intendono per:
a) "Radio Local Area Network (di seguito denominate "Radio LAN" o "R-LAN"): un sistema di comunicazioni in rete locale mediante radiofrequenze che utilizza apparati a corto raggio secondo le caratteristiche di armonizzazione e tecniche previste dal vigente Piano nazionale di ripartizione delle frequenze, nelle seguenti bande di frequenza: 2.400,0 – 2.483,5 MHz (brevemente banda a 2.4 GHz), 5.150 – 5.350 MHz, 5.470 – 5.725 MHz (brevemente bande a 5 GHz);
b) "access point" : strumento di accesso per un numero variabile di utenti tra la rete Radio-LAN e la struttura di rete di telecomunicazioni ;
c) "codici di abilitazione e identificazione": codici forniti dall'impresa autorizzata all'abbonato per identificarlo univocamente e verificarne l'abilitazione all'accesso alla rete tramite l'access point;
d) "autorizzazione generale": un'autorizzazione che è ottenuta su semplice dichiarazione di inizio attività.
2. Ai fini del presente decreto si applicano le definizioni di cui all'articolo 1, comma 1, del decreto del Presidente della Repubblica 19 settembre 1997, n. 318.

Art. 2
(Oggetto ed ambito di applicazione)

1. Il presente provvedimento fissa le condizioni per il conseguimento dell' autorizzazione generale per la fornitura, attraverso le applicazioni Radio LAN nella banda 2,4 GHz o nelle bande 5 GHz, dell'accesso del

pubblico alle reti e ai servizi di telecomunicazioni , in locali aperti al pubblico o in aree confinate a frequentazione pubblica quali aeroporti, stazioni ferroviarie e marittime e centri commerciali.
2. Ai fini della limitazione delle interferenze dannose ad altri servizi previsti dal Piano nazionale di ripartizione delle frequenze, gli access point operanti nella banda 5.150-5.350 MHz possono essere installati all'interno di edifici secondo le caratteristiche tecniche di cui alla nota 184 del Piano nazionale di ripartizione delle frequenze come modificato dal decreto del Ministro delle comunicazioni 20 febbraio 2003 , pubblicato nella Gazzetta Ufficiale n. 50 del 1° marzo 2003.

Art. 3

(Procedura per il conseguimento dell' autorizzazione generale)

1. La fornitura del servizio di cui all'articolo 2 è subordinata ad un'autorizzazione generale secondo le condizioni di cui all'articolo 6.
2. Il soggetto che intende fornire il servizio di cui all'articolo 2, avente sede in ambito nazionale o in uno dei paesi dello Spazio economico europeo (SEE), in uno dei paesi appartenenti all'Organizzazione mondiale del commercio (OMC), o in altri Paesi con i quali vi siano accordi di reciprocità nel settore disciplinato dal presente provvedimento, fatta comunque salva ogni eventuale limitazione derivante da accordi internazionali, è tenuto a presentare al Ministero delle comunicazioni, di seguito denominato "Ministero", una dichiarazione comprensiva di tutte le informazioni necessarie a verificare la conformità alle condizioni di cui all'articolo 6.
La predetta dichiarazione, che deve attenersi a quanto indicato nell'allegato A al presente decreto, costituisce denuncia di inizio attività e dà titolo ad avviare il servizio contestualmente alla sua presentazione.
3. Il soggetto richiedente allega alla dichiarazione la documentazione di cui all'art. 6, comma 1, lett. a) e b) della delibera dell'Autorità n. 467/00/Cons. Il soggetto che abbia precedentemente ottenuto una o più autorizzazioni all'offerta al pubblico di servizi di telecomunicazioni , può presentare la dichiarazione facendo riferimento alla documentazione già esibita, nei limiti della prevista validità.
4. I soggetti autorizzati sono obbligati all'iscrizione al registro degli operatori di comunicazione, previsto dall'articolo 1, comma 6, lett. a), n. 5), della legge 31 luglio 1997, n. 249, secondo le disposizioni della delibera dell'Autorità n. 236/01/Cons e successive modificazioni.
5. I soggetti che hanno presentato la dichiarazione di cui al presente articolo, comunicano entro 30 giorni al Ministero ogni variazione delle informazioni contenute nella stessa e nella relativa documentazione allegata.

Art. 4

(Contributi)

1. I diritti amministrativi imposti ai soggetti autorizzati ad offrire il servizio di cui all'articolo 2 coprono esclusivamente i costi amministrativi sostenuti per la gestione, il controllo e l'applicazione del regime di autorizzazione generale .
2. La misura di tali contributi sarà fissata con apposito provvedimento e resa pubblica ai sensi delle normative vigenti.

Art. 5

(Validità e cessione dell'autorizzazione generale)

1. L'autorizzazione generale di cui all'articolo 3 ha una durata non superiore a nove anni a decorrere dalla data di notifica della dichiarazione di cui al medesimo articolo ed è rinnovabile, previa nuova dichiarazione presentata con almeno trenta giorni di anticipo rispetto alla scadenza.
2. La scadenza coincide con il 31 dicembre dell'ultimo anno di validità dell'autorizzazione generale.
3. L'autorizzazione generale non può essere ceduta a terzi senza l'assenso del Ministero volto a verificare la sussistenza dei requisiti in capo all'impresa cessionaria, per il rispetto delle condizioni di cui all'autorizzazione medesima.

Art. 6

(Condizioni dell'autorizzazione generale)

1. Il soggetto titolare dell'autorizzazione generale per la fornitura, attraverso le applicazioni Radio LAN , dell'accesso del pubblico alle reti e ai servizi di telecomunicazioni , è tenuto a soddisfare le seguenti condizioni:

a) l'utilizzazione di apparecchiature conformi a quanto previsto dal decreto legislativo 9 maggio 2001, n. 268, di recepimento della direttiva 1999/5/CE;
b) la sicurezza delle operazioni di rete, il mantenimento dell'integrità della rete, l'interoperabilità dei servizi nonché la protezione dei dati; a tal fine l'interconnessione tra reti Radio LAN è ammessa esclusivamente attraverso reti pubbliche di telecomunicazioni ; è ammesso il collegamento tra gli access point appartenenti alla medesima Radio LAN limitatamente all'ambito geografico locale definito all'articolo 2, comma 1 e nel rispetto delle caratteristiche tecniche previste dal vigente Piano nazionale di ripartizione delle frequenze;
c) la fornitura delle informazioni necessarie per verificare il rispetto delle condizioni stabilite ed a fini statistici;
d) il rispetto della normativa vigente in materia di tutela della salute pubblica e dell'ambiente, ivi incluso il rispetto dei tetti previsti per le emissioni elettromagnetiche;
e) l'utilizzazione delle frequenze di cui all'articolo 1, comma 1, lett. a) esclusivamente secondo le caratteristiche di armonizzazione e tecniche previste dal vigente Piano nazionale di ripartizione delle frequenze, con l'esclusione di utilizzo delle medesime per scopi di interconnessione;
f) l'assenza di interferenze dannose alle altre utilizzazioni previste dal vigente Piano nazionale di ripartizione delle frequenze nelle bande di cui all'articolo 1, comma 1, lettera a), senza alcun diritto a protezione dalle medesime utilizzazioni ;
g) la pubblicizzazione delle condizioni di offerta del servizio, incluse quelle attinenti alle condizioni economiche, alla qualità e alla disponibilità del servizio nonché le relative variazioni delle condizioni stesse;
h) l'istituzione di una procedura per la trattazione dei reclami;
i) il pagamento dei contributi, ove previsti;
j) la fornitura di fatture dettagliate e documentate, ove applicabile in funzione della tipologia del servizio offerto;
k) l'adozione di opportuni codici di abilitazione e identificazione per identificare univocamente l'abbonato e verificarne l'abilitazione all'accesso alla rete tramite l'access point ;
l) il rispetto delle disposizioni vigenti in materia di pubblica sicurezza e tempestiva collaborazione con l'Autorità giudiziaria ai sensi dell'articolo 7, comma 13 del decreto del Presidente della Repubblica n. 318 del 1997;
m) il rispetto di ogni ragionevole misura tecnica di mitigazione, come previsto dalle rilevanti raccomandazioni e decisioni dell'ECC;
n) il rispetto delle eventuali disposizioni emanate dall'Autorità in materia di accesso, condivisione degli apparati e delle strutture, garanzie in materia di tutela della effettiva concorrenza.
2. In particolare il soggetto di cui al comma 1 è tenuto al rispetto degli obblighi di cui agli articoli 4 e 5 della direttiva 97/66/CE ed alle successive modificazioni di cui alla direttiva 2002/58/CE, quando recepita nell'ordinamento nazionale, che disciplinano gli aspetti legati alla sicurezza ed alla riservatezza delle reti e dei servizi.

Art. 7

(Controlli e verifiche - Disposizioni sanzionatorie-Conciliazione e risoluzione delle controversie)

1. Il Ministero e l'Autorità, nell'ambito delle rispettive competenze, possono procedere all'attuazione di controlli periodici per la verifica del rispetto delle condizioni di cui al presente decreto.
2. In caso di inosservanza delle condizioni previste per le autorizzazioni generali di cui al presente decreto si applicano le disposizioni di cui all'articolo 6, comma 4, del decreto del Presidente della Repubblica 19 settembre 1997, n. 318 e all'articolo 25 della legge 24 aprile 1998, n. 128, come modificato dall'articolo 13 della legge 21 dicembre 1999, n. 526.
3. Le procedure di conciliazione e risoluzione delle controversie sono disciplinate dall'articolo 18 del decreto del Presidente della Repubblica 19 settembre 1997, n. 318.

Art.8

(Disposizioni transitorie e finali)

1. Le imprese già autorizzate all'esercizio sperimentale del servizio di fornitura, attraverso le applicazioni Radio LAN, dell'accesso del pubblico alle reti e ai servizi di telecomunicazioni mediante l'impiego delle frequenze 2.400 – 2.483,5 MHz, cessano la sperimentazione entro sessanta giorni dalla entrata in vigore del presente decreto.

2. I titoli abilitativi di cui al presente decreto verranno adeguati alla normativa comunitaria in corso di recepimento di cui alle premesse, in materia di comunicazioni elettroniche.

Il presente decreto è pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

Sono state pubblicate le linee guida in materia di digitalizzazione dell' Amministrazione.

NUMERO SCHEDA: 2475

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: GAZZETTA UFFICIALE

DATA: 05/03/2003

NATURA ATTO: DIRETTIVA

DATA ATTO: 20/12/2002

ORGANO: MINISTERI

E' stata pubblicata la direttiva del Ministro per l'innovazione e le tecnologie 9 dicembre 2002 (G.U. n. 53 del 5-3-2003) che fornisce la linee guida in materia di digitalizzazione dell'Amministrazione, individuando le priorità che dovranno essere recepite nelle direttive dei vari Ministri per l'anno 2003 per digitalizzare le attività amministrative e i servizi resi ai cittadini e alle imprese.

I principali obietivi riguardano:

- l'adeguamento e l' armonizzazione dei Portali della pubblica amministrazione, anche in termini di accessibilità;
- l'incremento della presenza delle pubbliche amministrazioni in rete;
- la possibilità di'accesso esterno da parte dei cittadini per seguire le pratiche in modo da realizzare una maggiore trasparenza amministrativa;
- l'adozione di sistemi per l'autenticazione con carte di identità elettronica e carta nazionale dei servizi;
- l'accorpamento dei Centri elaborazione dati e creare strutture e sistemi unici che assicurino la continuità operativa.

Si riporta qui di seguito il testo della direttiva.

Dir.Min. 9 dicembre 2002

Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.

PREMESSA.

La presente direttiva è indirizzata a tutte le amministrazioni centrali dello Stato e agli enti pubblici sottoposti alla vigilanza ministeriale. Per le regioni e gli enti locali e territoriali costituisce contributo alle determinazioni in materia, nel rispetto della loro autonomia amministrativa. Può rappresentare schema di riferimento anche per le altre amministrazioni pubbliche di cui all'art. 1, comma 2, del *decreto legislativo 30 marzo 2001, n. 165*.
Il legislatore ha in questi anni emanato diverse norme volte a regolare gli aspetti concernenti la gestione elettronica dei documenti amministrativi per attuare la *legge n. 59 del 1997* che ha dato validità giuridica al documento informatico; tale attività normativa ha portato alla emanazione di norme disciplinanti sia la firma digitale (*decreto del Presidente della Repubblica n. 513 del 1997* e relative regole tecniche di cui al *decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999);* sia la tenuta dei sistemi di protocollo informatico (*decreto del Presidente della Repubblica n. 428 del 1998* e relative regole tecniche di cui al *decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000)*. Tali norme, ad eccezione di quelle recanti le citate «regole tecniche», sono poi confluite nel testo unico sulla documentazione amministrativa (*decreto del Presidente della Repubblica n. 445 del 2000)*. Ulteriori norme sono state emesse per garantire la interoperabilità dei sistemi di protocollo (Circolare 7 maggio 2001, n. AIPA/CR/28). Dal punto di vista della archiviazione del documento elettronico è stata emanata nel luglio del 1998 la deliberazione n. 24 del 1998 successivamente sostituita dalla deliberazione n. 42 del 2001; tale deliberazione si propone lo scopo di regolare la fase di conservazione dei documenti conformi alle normative precedentemente citate. Infine è stato emanato il *decreto legislativo 23 gennaio 2002, n. 10*, recante l'attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche che rende la normativa italiana sulla firma elettronica coerente con quella europea; fra le disposizioni citate si ritiene utile ricordare in particolare quelle concernenti i requisiti dei sistemi di cui agli articoli 52, 53, 55 e 56 del *decreto del Presidente della Repubblica n. 445 del 2000* ed all'art. 7 *decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000*.
Il *decreto del Presidente della Repubblica n. 445 del 2000* fissa al 1° gennaio 2004 il termine per la realizzazione dei sistemi finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi, lasciando a ciascuna amministrazione la scelta delle modalità organizzative e delle soluzioni tecnologiche da adottare.
Considerato il grande impatto sull'organizzazione delle amministrazioni ed in particolare sui sistemi di gestione dei flussi documentali è necessario che tutte le amministrazioni provvedano per tempo alla individuazione delle aree organizzative omogenee (art. 50 del *decreto del Presidente della Repubblica n. 445 del 2000)*, come peraltro richiamato dalla *Dir.Min. 21 dicembre 2001*, «Linee guida in materia di digitalizzazione dell'amministrazione» emanata dal Ministro per l'innovazione e le tecnologie, pubblicata nella Gazzetta Ufficiale - serie generale - del 5 febbraio 2002, n. 30, che ha sottolineato l'importanza del tema della trasparenza dell'azione amministrativa, intesa, in questo contesto, come concreto diritto del cittadino e dell'impresa di conoscere lo stato delle attività amministrative che li riguardano e avere la garanzia che tali attività siano condotte nel rispetto di regole di priorità e massimo impegno, nonché le opportunità che i sistemi di gestione del protocollo informatico offrono al riguardo.
Inoltre si ricorda che il Comitato dei Ministri per la Società dell'informazione ha approvato, il 13 febbraio 2002, un documento in cui sono stati definiti i dieci obiettivi fondamentali di legislatura, uno dei quali ha riguardato il tema della trasparenza dell'azione amministrativa. Tale obiettivo è coerente con il principio che l'azione delle amministrazioni debba essere guidata dalle esigenze degli utenti.
OBIETTIVI.
L'obiettivo primario di questa direttiva è quello di promuovere in tutte le amministrazioni centrali e gli enti pubblici sottoposti alla vigilanza ministeriale la realizzazione di sistemi informativi per la gestione elettronica dei flussi documentali.
Ciò allo scopo di assicurare il più rapido e proficuo utilizzo del documento informatico e della firma elettronica negli scambi di documenti ed atti tra amministrazioni, in coerenza con i rispettivi obiettivi istituzionali e con gli obiettivi strategici di digitalizzazione della pubblica amministrazione.
Il protocollo informatico e, più in generale, la gestione elettronica dei flussi documentali hanno la finalità di migliorare l'efficienza interna degli uffici attraverso l'eliminazione dei registri cartacei, la riduzione degli uffici di protocollo e la razionalizzazione dei flussi documentali. Inoltre con tali sistemi ci si prefigge di migliorare la trasparenza dell'azione amministrativa attraverso strumenti che consentano l'accesso allo stato dei procedimenti ed ai relativi documenti da parte di cittadini, imprese ed altre amministrazioni.

Per conseguire tali obiettivi è necessario che le amministrazioni, oltre ad ottemperare a quanto stabilito dalla normativa vigente (cd. «nucleo minimo», articoli 55 e 56 del *decreto del Presidente della Repubblica n. 445 del 2000)*, provvedano ad avviare progetti destinati a diffondere l'utilizzo di documenti elettronici sia al loro interno che negli scambi con i soggetti esterni, con lo scopo di facilitare e favorire l'accesso alle informazioni disponibili sui procedimenti e sui documenti protocollati.

INTEROPERABILITÀ E FLUSSI DOCUMENTALI.

L'azione coordinata di interventi che definiscono il quadro normativo e progettuale del nuovo sistema di gestione elettronica dei documenti ha prodotto:

la realizzazione da parte del Centro tecnico per la rete unitaria della pubblica amministrazione di un indice delle pubbliche amministrazioni (IPA) come previsto dal *decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000;* informazioni in proposito si trovano sul sito http//indicepa.gov.it;

la realizzazione di un sistema di posta elettronica certificata, cioè di un sistema che certifichi l'identificazione univoca del mittente e del destinatario e la ricezione del messaggio da parte di quest'ultimo, ai sensi del *decreto del Presidente della Repubblica n. 445 del 2000*, art. 14, allo scopo di fornire, nell'immediato, alle amministrazioni uno strumento sicuro di scambio di messaggi ufficiali e, in prospettiva, al cittadino e all'impresa un canale aggiuntivo di comunicazione con la pubblica amministrazione caratterizzato da rapidità ed efficienza.

Premesso che lo sviluppo di strumenti quali la firma elettronica ed il protocollo informatico, integrati con servizi di interoperabilità, rende possibile la realizzazione effettiva di una gestione completamente automatizzata dei flussi documentali, si ricorda che, nell'àmbito di una comunicazione tra i sistemi di protocollo di differenti amministrazioni, o tra differenti sistemi di protocollo della stessa amministrazione, si ritiene garantita la interoperabilità tra detti sistemi quando è consentito al sistema ricevente di trattare automaticamente le informazioni trasmesse dal sistema mittente.

Su tale tematica è possibile fare riferimento al testo del titolo «Interoperabilità dei sistemi di protocollo informatico in ambiente distribuito» emanato dall'Aipa e disponibile sul sito web http://protocollo.gov.it dedicato alla tematica oggetto della presente direttiva.

IMPLICAZIONI OPERATIVE PER LE AMMINISTRAZIONI.

Al fine di attuare la normativa vigente e usufruire dei servizi resi disponibili dal Centro tecnico, è necessario che le amministrazioni nei prossimi mesi svolgano un articolato insieme di azioni nell'àmbito della gestione elettronica dei documenti e della trasparenza amministrativa, azioni che sono di seguito descritte.

LA GESTIONE ELETTRONICA DEI DOCUMENTI.

Per i sistemi di gestione elettronica dei documenti è necessario:

individuare le aree organizzative omogenee (AOO) e i relativi uffici di riferimento ai sensi dell'art. 50, comma 4, del *decreto del Presidente della Repubblica n. 445 del 2000*;

comunicare al Centro tecnico la casella ufficiale di posta elettronica per l'iscrizione delle AOO nell'indice delle P.A.; indicazioni operative in tal senso saranno inviate dal Centro tecnico e sono presenti sul sito http://indicepa.gov.it;

comunicare al Centro tecnico, per ogni AOO istituita, il nominativo del responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61, comma 2, del *decreto del Presidente della Repubblica n. 445 del 2000*;

adottare, per ogni AOO istituita, il manuale di gestione come previsto dalle regole tecniche (art. 5 del *decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000*;)

pubblicare e rendere accessibile tramite internet il manuale di gestione che descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni necessarie per il corretto funzionamento del servizio per la tenuta del protocollo informatico. Il manuale comprende analisi, decisioni, piani, *iter* delle attività, classificazioni, ecc., definiti in relazione alle specificità organizzative, funzionali, strutturali e di servizio dell'amministrazione di riferimento; assumono particolare rilievo le disposizioni in merito alla pianificazione degli interventi, alla gestione ed all'*iter* di lavorazione dei documenti, dei sistemi di classificazione ed alle modalità di accesso;

predisporre un progetto operativo per la progressiva messa in opera di sistemi di protocollo informatico integrati con la posta elettronica certificata e la firma elettronica ai sensi dell'art. 10, comma 3, del *decreto del Presidente della Repubblica n. 445 del 2000* nel rispetto dei princìpi di interoperabilità di cui alla *circolare 7 maggio 2001, n. AIPA/CR/28*;

predisporre correlate attività di formazione d'intesa con il Dipartimento della funzione pubblica ai sensi della *Dir.Min. 13 dicembre 2001* del Ministro della funzione pubblica sulla formazione;
fornire informazioni al Centro tecnico sullo stato di avanzamento dei progetti al fine di permettere delle rilevazioni periodiche sullo stato di attuazione della normativa.
È necessario che le amministrazioni completino le attività precedentemente descritte entro il 31 maggio 2003.
A questo fine le amministrazioni in indirizzo definiscono un piano d'azione dettagliato che preveda lo svolgimento delle attività su elencate tenendo conto della scadenza del 1° gennaio 2004 prevista dal *decreto del Presidente della Repubblica n. 445 del 2000* per l'adozione del sistema di protocollo informatico e di comunicare, entro il 28 febbraio 2003, tale piano d'azione al Centro tecnico.
LA TRASPARENZA AMMINISTRATIVA.
Per l'attuazione della trasparenza dell'attività amministrativa, così come intesa da questa normativa, le amministrazioni svolgono, entro il 28 febbraio 2003, le seguenti azioni:
comunicare al Centro tecnico il nome di un referente, al fine di definire le attività di interesse comune e concordare i relativi tempi di realizzazione;
individuare i servizi di propria competenza erogati ai cittadini e alle imprese sia con modalità tradizionali che in rete;
pianificare, secondo criteri di priorità, l'attuazione della trasparenza dell'azione amministrativa come definita in precedenza, tramite la predisposizione di progetti orientati a fornire ai cittadini e alle imprese servizi informativi attraverso canali telematici diretti o tramite intermediazione dell'Ufficio relazioni con il pubblico;
migliorare la comunicazione tra gli uffici e gli URP al fine di migliorare la comunicazione esterna e l'esercizio del diritto di accesso;
compilare, per ogni progetto una scheda informativa, secondo lo schema riportato in allegato 1, da inviare al Centro tecnico. La scheda contiene gli elementi informativi essenziali per pianificare l'attuazione del progetto di trasparenza.
IL RUOLO DEL CENTRO TECNICO E DEL CENTRO DI COMPETENZA PER IL PROGETTO PROTOCOLLO INFORMATICO E TRASPARENZA AMMINISTRATIVA.
Il Centro tecnico, continuando le attività svolte fin qui dall'AIPA, ha istituito un centro di competenza per il progetto protocollo informatico e trasparenza amministrativa, quale unico punto di riferimento, che svolgerà funzioni di indirizzo e coordinamento e promuoverà iniziative di affiancamento per garantire l'attuazione della presente direttiva, in particolare attraverso:
le informazioni, le esperienze e i servizi messi a disposizione tramite il sito web sulla gestione elettronica dei documenti http://protocollo.gov.it;
la collaborazione che sarà fornita dal centro di competenza, che può essere contattato al seguente indirizzo di posta elettronica: protocollo@gov.it.

Disposizioni per l'informatizzazione della normativa vigente.

NUMERO SCHEDA: 2385

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: GAZZETTA UFFICIALE

DATA: 12/02/2003

NATURA ATTO: DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

DATA ATTO: 24/01/2003

E' stato pubblicato il decreto del Presidente del Consiglio dei Ministri datato 24 gennaio 2003 che, in attuazione dell'art. 107 della legge n. 388/2000 (legge finanziaria 2001) detta disposizioni per l'informatizzazione della normativa vigente.
L'art. 107 citato ha istituito presso la Presidenza del Consiglio dei Ministri un fondo destinato al finanziamento di iniziative volte a promuovere l'informatizzazione e la classificazione della normativa vigente al fine di facilitarne la ricerca e la consultazione gratuita da parte dei cittadini, nonche' di fornire strumenti per l'attivita' di riordino normativo.
Il decreto in argomento ha poi definito il programma, le forme organizzative e le modalita' di funzionamento del fondo in esecuzione di quanto previsto dalla stessa disposizione legislativa di carattere generale. Tale programma tiene conto dei suggerimenti dell'AIPA che, con la circolare n. 40 del 22 aprile 2002, aveva indicato le regole da rispettare nell'esercizio dell'attivita' di drafting (tecniche di redazione dei provvedimenti). L'Autorita' facendo riferimento a precedenti provvedimenti della Presidenza del Consiglio dei Ministri (in particolare la circolare del 20 aprile 2001) e prendendo le mosse dal programma e-Europe, aveva ribadito la necessita' di intraprendere iniziative idonee a consentire l'accessibilita' telematica alle norme, risolvendo i problemi di carattere giuridico e tecnologico.
Il decreto in esame individua le attività costituenti il programma delle iniziative di cui citato art.107, le forme organizzative e le modalità di finanziamento a valere sul fondo di cui alla predetta disposizione.
In particolare il programma di informatizzazione prevede:

- una compilazione ragionata del testo delle leggi statali e degli altri atti normativi emanati dallo Stato;
- la messa a disposizione gratuita, con strumenti informatici e telematici dei testi citati;
- una classificazione della normativa vigente secondo parametri per favorire la ricerca per via informatica e telematica;
- lo studio e l'applicazione di strumenti e procedure di ricerca raffinata della normativa vigente;
- lo studio e l'applicazione di sistemi avanzati di trattamento informatico, di marcatura e di classificazione degli atti normativi, anche ai fini dell'istruttoria dell'attivita' di riordino normativo;
- la realizzazione di appositi portali e siti Internet, corredati da idonei motori di ricerca, ai fini delle attivita' di cui in precedenza

Si riporta di seguito il testo del decreto.

D.P.C.M. 24 gennaio 2003

Disposizioni per l'informatizzazione della normativa vigente, in attuazione dell'art. 107 della *L. 23 dicembre 2000, n. 388.*

1. Oggetto.

1. Il presente decreto individua le attività costituenti il programma delle iniziative di cui all'art. 107 della *legge 23 dicembre 2000, n. 388*, le forme organizzative, nonché le modalità di finanziamento a valere sul fondo di cui alla predetta disposizione.

2. Contenuto del programma.

1. Rientrano nel programma di cui all'art. 1 le seguenti attività:

a) compilazione del testo delle leggi statali e degli altri atti normativi emanati dallo Stato, quale risultante dalle modifiche e abrogazioni espresse;

b) messa a disposizione gratuita, con strumenti informatici e telematici, dei testi di cui alla lettera *a*), e delle relazioni afferenti al singolo atto normativo;

c) classificazione della normativa vigente di cui alla lettera *a*) secondo parametri per favorire la ricerca per via informatica e telematica, nonché predisposizione di un idoneo apparato critico atto ad individuare profili di incompatibilità ed abrogazioni implicite fra disposizioni;

d) studio ed applicazione di strumenti e procedure di ricerca raffinata della normativa vigente, nonché di sistemi avanzati di trattamento informatico, di marcatura e di classificazione degli atti normativi, anche ai fini dell'istruttoria dell'attività di riordino normativo;

e) realizzazione di appositi portali e siti Internet, corredati da idonei motori di ricerca, ai fini delle attività di cui alle lettere precedenti.

2. Le attività incluse nel programma sono definite in coordinamento con le iniziative già avviate nel campo della informatizzazione della documentazione giuridica pubblica, in particolare dalla Corte costituzionale, dalla Corte suprema di cassazione, dalla Magistratura amministrativa e contabile, dal Ministero della giustizia, dall'Istituto Poligrafico e Zecca della Stato, dall'AIPA, dalle regioni e dalle province autonome.

3. Con protocolli di intesa, approvati dal Comitato guida di cui all'art. 4, stipulati tra la Presidenza del Consiglio dei Ministri e le regioni, si stabiliscono modalità e termini di partecipazione delle regioni al programma ovvero di coordinamento delle iniziative di competenza.

4. In conformità alle determinazioni e valutazioni espresse dal citato comitato guida, la Presidenza del Consiglio dei Ministri approva i progetti ammessi al finanziamento e può, altresì, stipulare convenzioni con soggetti pubblici e privati che intendono finanziare con proprie risorse attività previste nel programma o che intendono attuare direttamente con proprie risorse progetti o parti di essi, rientranti nel programma medesimo.

3. Attuazione del programma.

1. Il programma è realizzato mediante progetti proposti dagli organi costituzionali, dalla Presidenza del Consiglio dei Ministri, dalle altre pubbliche amministrazioni di cui all'art. 1, comma 2, del *decreto legislativo 30 marzo 2001, n. 165*, e successive modificazioni, nonché da soggetti privati o anche da soggetti appositamente costituitisi in collaborazione tra enti pubblici e privati.

4. Comitato guida.

1. È costituito un Comitato guida, formato dai segretari generali della Camera dei deputati, del Senato della Repubblica e della Presidenza del Consiglio dei Ministri o da loro delegati.

2. Il Comitato guida procede d'intesa sulla base delle direttive del Presidente del Consiglio dei Ministri, del Presidente della Camera dei deputati e del Presidente del Senato della Repubblica, a:

a) determinare gli indirizzi generali per l'attuazione del programma;

b) definire gli obiettivi e la cadenza temporale per la realizzazione del programma di cui all'art. 2;

c) definire i requisiti di ammissione al programma dei progetti di cui all'art. 3;

d) definire le modalità e i termini per la redazione e la presentazione di progetti di implementazione del programma;

e) valutare la conformità agli obiettivi del programma dei progetti ammissibili a finanziamento da parte del fondo;

f) verificare lo stato di attuazione del programma e riferirne ai Presidenti delle Camere e al Presidente del Consiglio dei Ministri con cadenza almeno annuale.

3. L'attività preparatoria delle determinazioni del Comitato guida è curata dal Dipartimento per gli affari giuridici e legislativi della Presidenza del Consiglio dei Ministri tramite un gruppo di lavoro operante presso il Segretariato generale della Presidenza del Consiglio dei Ministri, costituito da personale designato dalla Presidenza del Consiglio dei Ministri, dalla Camera dei deputati e dal Senato della Repubblica. I compiti di esecuzione del programma sono attribuiti, nell'àmbito delle rispettive competenze, al

Dipartimento per gli affari giuridici e legislativi nonché al Dipartimento per l'innovazione e le tecnologie ed alle altre strutture di cui si avvale il Ministro per l'innovazione e le tecnologie.
4. Il Comitato guida può procedere, anche tramite il gruppo di lavoro, a consultazioni di soggetti pubblici e privati interessati al tema della conoscibilità della normazione.
5. Modificazioni al presente decreto.
1. Eventuali modificazioni al presente decreto sono disposte con la forma e nel rispetto della procedura stabilite dall'art. 107 della *legge 23 dicembre 2000, n. 388*.

La legge finanziaria 2003 (legge 27 dicembre 2002, n. 289) ha istituito il Fondo per il finanziamento di progetti di innovazione tecnologica nelle pubbliche amministrazioni.

NUMERO SCHEDA: 2167

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

NATURA ATTO: LEGGE

DATA ATTO: 27/12/2002

NUM. ATTO: 289

L'articolo 26 della legge n. 289/2002, recante "Disposizioni in materia di innovazione tecnologica", istituisce il Fondo per il finanziamento di progetti di innovazione tecnologica nelle pubbliche amministrazioni e nel Paese.
Il Ministro per l'innovazione e le tecnologie, di concerto con il ministro per la funzione pubblica e il Ministro dell'economia e delle finanze, con uno o più decreti:
- stabilisce le modalità di funzionamento del Fondo;
- individua i progetti da finanziare;
- individua, ove necessario, la relativa ripartizione tra le amministrazioni interessate.

Si allega il testo dell'articolo.

Articolo 26
(Disposizioni in materia di innovazione tecnologica)
1. Per l'attuazione del comma 7 dell'articolo 29 della legge 28 dicembre 2001, n. 448, è istituito il Fondo per il finanziamento di progetti di innovazione tecnologica nelle pubbliche amministrazioni e nel Paese con una dotazione di 100 milioni di euro per l'anno 2003, al cui finanziamento concorrono la riduzione dell'8 per cento degli stanziamenti per l'informatica iscritti nel bilancio dello Stato e quota parte delle riduzioni per consumi intermedi di cui all'articolo 23, comma 3. Il Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e il Ministro dell'economia e delle finanze, con uno o più decreti di natura non regolamentare, stabilisce le modalità di funzionamento del Fondo, individua i progetti da finanziare e, ove necessario, la relativa ripartizione tra le amministrazioni interessate.
2. Al fine di assicurare una migliore efficacia della spesa informatica e telematica sostenuta dalle pubbliche amministrazioni, di generare significativi risparmi eliminando duplicazioni e inefficienze, promuovendo le migliori pratiche e favorendo il riuso, nonché di indirizzare gli investimenti nelle tecnologie informatiche e telematiche, secondo una coordinata e integrata strategia, il Ministro per l'innovazione e le tecnologie:

a) definisce con proprie direttive le linee strategiche, la pianificazione e le aree di intervento dell'innovazione tecnologica nelle pubbliche amministrazioni, e ne verifica l'attuazione;

b) approva, con il Ministro dell'economia e delle finanze, il piano triennale ed i relativi aggiornamenti annuali di cui all'articolo 7 del decreto legislativo 12 febbraio 1993, n. 39, entro il 30 giugno di ogni anno;

c) valuta la congruenza dei progetti di innovazione tecnologica che ritiene di grande valenza strategica rispetto alle direttive di cui alla lettera a) ed assicura il monitoraggio dell'esecuzione;

d) individua i progetti intersettoriali che devono essere realizzati in collaborazione tra le varie amministrazioni interessate assicurandone il coordinamento e definendone le modalità di realizzazione;

e) valuta, sulla base di criteri e metodiche di ottimizzazione della spesa, il corretto utilizzo delle risorse finanziarie per l'informatica e la telematica da parte delle singole amministrazioni;

f) stabilisce le modalità con le quali le pubbliche amministrazioni comunicano le informazioni relative ai programmi informatici, realizzati su loro specifica richiesta, di cui esse dispongono, al fine di consentirne il riuso previsto dall'articolo 25, comma 1, della legge 24 novembre 2000, n. 340;

g) individua specifiche iniziative per i comuni con popolazione inferiore a 5.000 abitanti e per le isole minori;

h) promuove l'informazione circa le iniziative per la diffusione delle nuove tecnologie.

3. Nei casi in cui i progetti di cui ai commi 1 e 2 riguardino l'organizzazione e la dotazione tecnologica delle regioni e degli enti territoriali, i provvedimenti sono adottati sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281.

4. Al fine di accelerare la diffusione della carta di identità elettronica e della carta nazionale dei servizi, le pubbliche amministrazioni interessate, nel quadro di un programma nazionale approvato con decreto dei Ministri per l'innovazione e le tecnologie, dell'economia e delle finanze, della salute e dell'interno, possono procurarsi i necessari finanziamenti nelle seguenti forme anche cumulabili tra loro:

a) convenzioni con istituti di credito o finanziari;

b) contributi di privati interessati a forme di promozione;

c) ricorso alla finanza di progetto;

d) operazioni di cartolarizzazione.

5. Con decreto del Ministro dell'istruzione, dell'università e della ricerca, adottato di concerto con il Ministro per l'innovazione e le tecnologie, sono determinati i criteri e le procedure di accreditamento dei corsi universitari a distanza e delle istituzioni universitarie abilitate a rilasciare titoli accademici, ai sensi del regolamento di cui al decreto del Ministro dell'università e della ricerca scientifica e tecnologica 3 novembre 1999, n. 509, al termine dei corsi stessi, senza oneri a carico del bilancio dello Stato. Ai fini dell'acquisizione dell'autorizzazione al rilascio dei titoli accademici, le istituzioni devono disporre di adeguate risorse organizzative e gestionali in grado di:

a) presentare un'architettura di sistema flessibile e capace di utilizzare in modo mirato le diverse tecnologie per la gestione dell'interattività, salvaguardando il principio della loro usabilità;

b) favorire l'integrazione coerente e didatticamente valida della gamma di servizi di supporto alla didattica distribuita;

c) garantire la selezione, progettazione e redazione di adeguate risorse di apprendimento per ciascun courseware;

d) garantire adeguati contesti di interazione per la somministrazione e la gestione del flusso dei contenuti di apprendimento, anche attraverso l'offerta di un articolato servizio di teletutoring;

e) garantire adeguate procedure di accertamento delle conoscenze in funzione della certificazione delle competenze acquisite; provvedere alla ricerca e allo sviluppo di architetture innovative di sistemi e-learning in grado di supportare il flusso di dati multimediali relativi alla gamma di prodotti di apprendimento offerti.

6. Per la realizzazione dell'anagrafe degli italiani residenti all'estero e per la informatizzazione delle prefetture è autorizzata la spesa di 25 milioni di euro per ciascuno degli anni 2003, 2004 e 2005.

Linee guida del Governo per lo sviluppo della Società dell'Informazione nella legislatura. - Ruolo delle regioni nel processo innovativi della Pubblica Amministrazione.

NUMERO SCHEDA: 1657

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: MINISTERI

DATA: 30/06/2002

DATA ATTO: 30/06/2002

Il Ministro per l'Innovazione e le Tecnologie ha diffuso un importante documento, intitolato "Linee guida del Governo per lo sviluppo della Società dell'Informazione nella legislatura" che definisce l'impegno del Governo nella modernizzazione della P.A. attraverso un utilizzo diffuso delle nuove tecnologie ICT (Tecnologie dell'Informazione e delle Comunicazione) sia nel pubblico che nel privato. L' evoluzione delle tecnologie porterà, infatti, a significativi impatti su cittadini, imprese e Pubbliche Amministrazioni. Per la P.A. determinerà, in particolare:

- facilità di entrare in contatto e fornire servizi al cittadino;
- miglioramento dei canali di comunicazione tra le Amministrazioni, che consentirà maggior efficienza delle stesse;
- ottimizzazione dell'uso delle risorse pubbliche attraverso l'applicazione delle tecnologie.

Per favorire la ricerca applicata nei diversi settori dell'ICT, il Dipartimento per l'innovazione e le tecnologie ha individuato, in collaborazione con il Ministero dell'Istruzione Università e Ricerca e il Ministero delle Attività Produttive, alcune linee di azione sinergiche.

La tecnologia dell'informazione e della comunicazione riveste un ruolo fondamentale anche nel percorso di attuazione del federalismo, che prevede una cooperazione puntuale tra le amministrazioni, poiché consente, quale strumento di coordinamento tra i diversi oggetti istituzionali, un miglioramento dei servizi ed un progressivo superamento della frammentazione della P.A.. In tale ambito le regioni rivestono un ruolo decisivo nella pianificazione, programmazione ed attuazione dei processi innovativi della P.A.. Il documento, nella parte II, relativa a "La trasformazione della Pubblica Amministrazione" ne sottolinea l'importanza strategica nel processo di eGovernment.

Per consultare il testo:
http://www.giurdanella.net/file_sito/min_inn_tec_lineeguida2002.pdf

In Gazzetta la direttiva sulla informatizzazione della p.a.

NUMERO SCHEDA: 1063

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: ITALIA OGGI

AUTORE: F. Cerisano

NUMERO: 32

DATA: 07/02/2002

PAGINA: 39

NATURA ATTO: DIRETTIVA

DATA ATTO: 21/12/2001

E' stata pubblicata sulla Gazzetta Ufficiale n. 30 del 5 febbraio 2002 la direttiva "Linee guida in materia di digitalizzazione dell'amministrazione", adottata il 21 dicembre 2001 dal ministro per l'innovazione tecnologica, il cui testo è a disposizione.
La direttiva recepisce "la volontà del Governo di avviare un vero processo di cambiamento della pubblica amministrazione", fissando obiettivi concreti per il conseguimento dei quali "le leve dell'innovazione e della tecnologia si configurano quali fattori imprescindibili e distintivi".
Ecco alcuni punti affrontati nella direttiva.
Flussi documentali: ogni comunicazione interna sarà inviata ai destinatari in formato digitale, utilizzando i sistemi presenti nelle varie amministrazioni.
Realizzazione del portale nazionale "e-Italia": si tratterà di un sito con tutte le informazioni sul funzionamento dello stato e delle amministrazioni periferiche con lo scopo di indirizzare il cittadino verso i servizi dei quali ha necessità.
Acquisto di beni e servizi: tutte le attività di acquisizione di beni e di servizi saranno svolte per via elettronica.
Contabilità: sarà effettuata per via elettronica e i documenti approvati per via elettronica.
Gestione del personale: anch'essa sarà informatizzata.
Postazione di lavoro informatizzata: sarà necessaria per la maggior parte dei dipendenti pubblici.
Carta multiservizi del dipendente: dotata di microcircuito che contenga la firma digitale sarà adibita a svariati usi (controllo accessi, firma digitale, identificazione ecc.).
E-learning: diffusione delle tecniche di formazione a distanza.

Si allega il testo della direttiva.

Dir.Min. 21 dicembre 2001

Linee guida in materia di digitalizzazione dell'amministrazione

1. Premessa.
Le presenti linee guida del Ministro per l'innovazione e le tecnologie recepiscono la volontà del Governo di avviare un vero processo di cambiamento della pubblica amministrazione e fissano obiettivi concreti, mirati e misurabili, per il cui conseguimento le leve dell'innovazione e della tecnologia si configurano quali fattori imprescindibili e distintivi.
Le linee guida costituiscono indirizzi per le amministrazioni dello Stato ed integrano i piani da queste già definiti per l'anno 2002, individuando le priorità di intervento dell'ampio progetto di rinnovamento della pubblica amministrazione, promosso dal Governo.
L'obiettivo delle presenti linee guida è l'attivazione, già a partire dall'anno 2002, di un processo di cambiamento, che consenta un rapido, visibile e misurabile sviluppo dell'innovazione e dell'utilizzo delle tecnologie nelle amministrazioni dello Stato.
Le linee guida del presente documento si inseriscono in un contesto più ampio, caratterizzato anche, nell'àmbito del programma complessivo del Governo, dalle finalità di:
condurre il Paese in una posizione di leadership nell'era digitale;
supportare la modernizzazione del Paese attraverso la realizzazione di un nuovo modello di Stato informatizzato e digitalizzato;
favorire l'avvento dell'economia di rete rendendo disponibili on line i servizi pubblici ai cittadini ed alle imprese;
disegnare una strategia per l'innovazione e le tecnologie basata su una visione unitaria ed articolata secondo uno schema di azione chiaro e strutturato.
In particolare, le linee guida per l'anno 2002 costituiscono un primo gruppo di obiettivi prioritari che dovranno essere realizzati nel corso del prossimo esercizio e che verranno recepiti ed estesi nell'àmbito di un piano strategico per l'innovazione e le tecnologie, per il periodo 2002 - 2004, attualmente in corso di predisposizione.
Gli interventi previsti per l'anno 2002 si pongono tre ambiziosi obiettivi:
favorire la creazione dei presupposti interni alle amministrazioni, in termini di norme, organizzazione, processi e tecnologie, per migliorare il livello dei servizi offerti al cittadino ed alle imprese e per incrementare l'efficienza dei processi interni;
contribuire alla qualificazione del personale della pubblica amministrazione e valorizzare l'investimento in capitale umano, attraverso l'innovazione ed un coinvolgimento diretto al processo di cambiamento in atto;
valorizzare il ruolo della pubblica amministrazione come promotore della economia di rete, aggregatore della domanda di innovazione e volano per lo sviluppo del mercato delle nuove tecnologie in Italia.
Gli interventi promossi sono coerenti con l'evoluzione dell'assetto istituzionale del Paese, in termini di orientamento al decentramento e di rispetto della autonomia delle amministrazioni.
2. Indirizzi prioritari.
Gli indirizzi prioritari della presente direttiva si riferiscono alle seguenti direttrici di intervento principali, che dovranno qualificare le direttive generali di ciascun Ministro:
migliorare il livello di servizio ai cittadini ed alle imprese, attraverso l'attivazione di punti unici di contatto con le amministrazioni, l'abilitazione di strumenti di identificazione del cittadino e la realizzazione di interventi organizzativi che supportino tali interventi e garantiscano la trasparenza dell'azione amministrativa (Uffici digitali, Portale nazionale del cittadino, ecc.);
favorire l'efficienza e l'economicità di gestione, attraverso la promozione di interventi integrati di cambiamento normativo, ridisegno dei processi, introduzione di nuove soluzioni tecnologiche e ricorso a strumenti di gestione del cambiamento (metodologie di gestione progetto; acquisti di beni e servizi; gestione della contabilità finanziaria ed economica; gestione del personale; flussi documentali);
potenziare l'attuale infostruttura, avviando il lancio di iniziative progettuali e normative volte a favorire lo sviluppo di un efficiente contesto informativo interno alle amministrazioni dello Stato, orientato alla

condivisione dei servizi e delle informazioni fra le amministrazioni attraverso le tecnologie (sicurezza; postazione di lavoro informatizzata; carta multiservizi del dipendente; valorizzazione del patrimonio informativo esistente);
sviluppare le competenze informatiche e tecnologiche dei dipendenti dello Stato, attraverso l'avvio di un ampio progetto di formazione e gestione del cambiamento che preveda un focus specifico sull'alfabetizzazione tecnologica, sull'apprendimento della lingua inglese e sull'utilizzo di Internet mediante il ricorso a tecniche di formazione a distanza (e-learning);
promuovere la diffusione dell'innovazione nel Paese, attraverso alcune grandi iniziative di rilevanza nazionale che abbiano un impatto significativo sul Paese, che prevedano l'aggregazione della domanda pubblica di innovazione e favoriscano lo sviluppo della Società dell'informazione nel Paese («iniziativa larga banda»; sviluppo di servizi digitali su larga banda; e-commerce);
introdurre strumenti innovativi di coordinamento e gestione delle iniziative, mediante l'avvio di gruppi di lavoro congiunti fra il Dipartimento per l'innovazione e le tecnologie e le amministrazioni per la pianificazione, la realizzazione ed il monitoraggio degli interventi comuni, prevedendo in quest'ultimo caso anche il coinvolgimento dei servizi di controllo interno delle singole amministrazioni e dei referenti designati dalle singole amministrazioni a seguito della lettera a tutti i Ministri del Ministro per l'innovazione e le tecnologie del 28 giugno 2001.
3. Programmi per il 2002.
3.1. Migliorare il livello di servizio.
Le amministrazione statali hanno tutte una maggiore o minore, a seconda dei casi, attività di interazione con i cittadini e con le imprese.
Al fine di dare attuazione agli strumenti già introdotti (firma elettronica, protocollo informatizzato), nel corso del 2002 dovranno essere avviati programmi di utilizzo di tali strumenti per una più completa espansione nel 2003/2004.
Occorre infatti dare una maggiore trasparenza ai cittadini relativamente alle istanze/richieste di informazioni presentate alle amministrazioni dello Stato.
L'obiettivo del 2002 dovrà quindi essere quello di consentire che ogni cittadino possa inviare istanze o domande utilizzando diverse tecnologie e canali alternativi (Internet, call center, chioschi digitali).
Le richieste dovranno essere veicolate verso un unico punto di contatto con il cittadino dove saranno protocollate e, per quanto possibile, processate elettronicamente.
Flussi documentali
Al fine di potenziare l'uso della posta elettronica, ogni comunicazione interna sarà inviata ai destinatari in formato digitale, utilizzando i sistemi in essere presso le varie amministrazioni.
Per avviare concretamente tali procedure, sarà svolta nel 2002, con il coordinamento del Dipartimento per l'innovazione e le tecnologie e la collaborazione di un primo insieme di amministrazioni, una prima fase transitoria di sperimentazione. Nel corso della fase transitoria le amministrazioni verificheranno le proprie dotazioni informatiche, al fine di prepararsi alla realizzazione di tale iniziativa nell'ottica della trasparenza e del servizio al cittadino.
Le amministrazioni dovranno individuare al loro interno le aree organizzative omogenee, le quali, dotate di un sistema di protocollo informatico, potranno ricevere da cittadini, imprese o altre amministrazioni sia documenti in formato elettronico, sia documenti cartacei che saranno smaterializzati tramite scanner.
I documenti registrati dal sistema di protocollo informatico saranno poi distribuiti per via telematica agli uffici competenti all'interno della struttura organizzativa facente parte dell'area organizzativa omogenea.
Gli interventi citati si inseriscono in un complessivo processo di rinnovamento delle modalità e degli strumenti per la gestione dei flussi documentali. In particolare, alla luce degli obiettivi di efficienza e trasparenza dei processi amministrativi, la digitalizzazione dei flussi di documentazione interna strutturata e l'introduzione del protocollo informatico risultano cruciali, in quanto consentono lo snellimento, la tracciabilità ed il monitoraggio continuo dei documenti da parte degli utenti.
La previsione di cui al testo unico n. 445/2000, obbliga le amministrazioni a realizzare entro il 1° gennaio 2004 il solo «Nucleo minimo», definendo in tal modo tempi lunghi per obiettivi limitati, rispetto al livello di innovazione raggiungibile con una completa attuazione di tutte le componenti, in particolare quella relativa alla trasparenza, l'unica concretamente visibile al cittadino e all'impresa.
È quindi necessario che, nella pianificazione della attività per l'anno 2002, si seguano precise guide di ordine tecnico ed organizzativo per accelerare ed ampliare gli obiettivi realizzativi. È perciò necessario che

ciascuna amministrazione individui strutture o gruppi di lavoro cui affidare la responsabilità della attuazione di questo progetto.
Si ritiene, infine, che particolare attenzione possa essere rivolta dalle amministrazioni nel tener conto di questo progetto per operare una riqualificazione del personale disabile mediante l'uso di opportune tecnologie assistive.
Ufficio digitale
In attesa della completa applicazione dell'automazione dei flussi documentali e per verificarne l'efficacia, il Dipartimento per l'innovazione e le tecnologie studierà, di concerto con il Dipartimento della funzione pubblica, la possibilità di introdurre in via sperimentale l'Ufficio digitale, intendendo come tale un'unità in cui le amministrazioni, dopo avere selezionato pochi ma efficaci servizi di particolare importanza e visibilità per il cittadino, potranno processarli elettronicamente tramite sistemi di gestione di flussi documentali. In tali uffici digitali saranno il più possibile concentrate le competenze e responsabilità per completare l'iter di erogazione dei servizi stessi in modo elettronico, dando ampia trasparenza e visibilità nonché consentendo una drastica riduzione dei tempi amministrativi. Tali uffici vanno intesi come moduli di raccordo tra gli uffici competenti e non come strutture aggiuntive rispetto all'ordinamento organizzativo vigente. Ad esempio, la sperimentazione potrà partire dalle iniziative in corso per la realizzazione degli uffici relazioni con il pubblico e degli sportelli unici per le attività produttive, per renderli completamente operanti secondo modalità elettroniche.
Quanto sopra richiederà un'azione di semplificazione, ove necessario normativa, che renda possibile tale trasparenza, nonché azioni organizzative interne per attuare tali iniziative.
Sarà compito delle amministrazioni definire di concerto con il Dipartimento per l'innovazione e le tecnologie ed il Dipartimento della funzione pubblica i servizi «pilota» da avviare nel corso del 2002.
In tale contesto il cittadino potrà inviare la propria istanza identificandosi mediante strumenti di identificazione elettronica, quali la Carta di identità elettronica o la Carta nazionale dei servizi; qualora non possegga ancora tali strumenti, potrà ricorrere alla sola firma elettronica.
L'intervento potrà includere la realizzazione di collegamenti con le amministrazioni periferiche dello Stato, con le quali le amministrazioni centrali si interfacciano.
Portale nazionale
È obiettivo del Dipartimento per l'innovazione e le tecnologie avviare, nell'àmbito del piano di e-government, la realizzazione del portale nazionale «e-Italia». Tale iniziativa costituirà un punto di aggregazione delle informazioni relative al funzionamento dello Stato, agli iter procedurali della pubblica amministrazione ed alle modalità di erogazione dei servizi alla collettività, oltre a rappresentare una porta di accesso unificato ai servizi digitali resi disponibili dalle diverse strutture amministrative pubbliche.
In particolare, il portale «e-Italia» presenterà caratteristiche e funzionalità che ne qualificano l'offerta di servizio:
organizzazione dei contenuti informativi ospitati secondo uno schema logico che ripercorre i principali episodi della vita del cittadino;
indirizzamento «intelligente» ai servizi digitali offerti dalla pubblica amministrazione centrale e locale;
composizione di una vetrina di contenuti organizzati per aree tematiche, trasversali rispetto agli episodi della vita, relative alle nuove tecnologie e alla società digitale (notizie e forum di discussione su Carta nazionale dei servizi, Carta d'identità elettronica, Rapporti sulla società dell'informazione, ecc.);
predisposizione di un «indirizzario» delle pubbliche amministrazioni («Pagine gialle») e di un motore di ricerca dei contenuti residenti nel portale e nei siti attivati da tutte le amministrazioni;
abilitazione all'utilizzo di strumenti evoluti di interazione e transazione con la pubblica amministrazione quali la firma digitale, la Carta nazionale dei servizi, la Carta d'identità elettronica, le carte di pagamento.
La realizzazione del portale «e-Italia» risponde all'obiettivo ultimo di trasmettere al cittadino una visione unitaria e facilmente accessibile della pubblica amministrazione, configurandosi altresì quale strumento di cooperazione tra le diverse amministrazioni.
Al fine di rendere possibile il pieno funzionamento dell'iniziativa nell'ottica descritta, le varie amministrazioni dovranno fornire il proprio contributo per rendere disponibili i contenuti di propria competenza nel portale, garantendone il continuo aggiornamento e monitoraggio.
Alla luce, inoltre, della necessità di erogare la più ampia gamma di servizi digitali integrati ai cittadini, le singole amministrazioni sono chiamate ad agevolare la realizzazione delle soluzioni tecnologiche di integrazione del portale con i propri siti Internet.

La collaborazione tra le amministrazioni dovrà essere supportata dalla costituzione, nel corso del 2002, di gruppi di lavoro comuni, la cui attività sarà orientata alla interpretazione delle esigenze dei cittadini ed alla predisposizione delle migliori risposte.
Inoltre, un obiettivo da conseguire in tempi rapidi è quello di rivedere i siti Internet prevalentemente informativi delle varie amministrazioni, per renderli più vicini ai cittadini ed in grado di fornire notizie anche di attualità ed in tempo reale, riguardanti l'amministrazione. Bisognerà privilegiare siti «interattivi», tali da consentire lo scambio bidirezionale di informazioni tra amministrazioni e cittadini, ad esempio la creazione di forum di comunità di utenti interessati ad argomenti specifici.
A tal fine, il Dipartimento per l'innovazione e le tecnologie definirà standards tecnici e grafici che facilitino l'individuazione di una immagine distintiva della pubblica amministrazione nei riguardi del cittadino e delle imprese.
Entro il 31 gennaio del 2002, ogni amministrazione dovrà nominare un proprio responsabile del sito per partecipare al programma di cambiamento.
3.2. Favorire l'efficienza e l'economicità di gestione.
L'incremento dell'efficienza interna delle amministrazioni è legato ad un approccio integrato che prevede un profondo cambiamento dei processi interni, un forte ricorso alle tecnologie ed alla innovazione, l'avvio di specifici piani di formazione e gestione del cambiamento.
In particolare, gli interventi di razionalizzazione dovranno riguardare sia i processi comuni a tutte le amministrazioni, sia alcuni processi specifici tipici delle diverse amministrazioni. L'anno 2002 prevede anche una focalizzazione sul miglioramento dei processi di back office comuni alle diverse amministrazioni (contabilità e «mandato informatico», gestione del personale, acquisti «on line» di beni e servizi).
Metodologie di gestione progetto
Il conseguimento di un significativo miglioramento dell'efficienza interna delle amministrazioni è condizionato dall'avvio, nel corso dell'anno 2002, di importanti progetti di riorganizzazione, che prevedono un ridisegno dei processi interni ed un forte ricorso alle nuove tecnologie.
L'adozione di metodologie comuni alle amministrazioni, che consentano un «approccio standard» ai progetti per il miglioramento dell'efficienza, è un requisito importante per il successo di tali iniziative.
In particolare tutti i progetti di miglioramento, che saranno avviati nel corso del 2002, dovranno prevedere:
la preventiva esecuzione di uno studio di fattibilità che definisca gli obiettivi, le attività, i costi, i benefici ed i tempi di realizzazione, e che espliciti i conseguenti interventi di ridisegno organizzativo;
specifiche attività di riorganizzazione dei processi e di ricorso alle nuove tecnologie;
il ricorso a strumenti di gestione del cambiamento (formazione, comunicazione, ecc.) finalizzati a massimizzare l'efficacia del progetto;
l'attivazione di strumenti per il monitoraggio dei risultati;
la valutazione del possibile riuso di progetti/soluzioni già esistenti;
l'evidenziazione dei «ritorni» di ciascun investimento informatico (indicazione dei benefici, misurabili);
le penali da applicare ai soggetti privati che eventualmente collaboreranno alla realizzazione del progetto, in caso di non raggiungimento dei risultati previsti.
Inoltre il Dipartimento per l'innovazione e le tecnologie in collaborazione con il Ministro per l'attuazione del programma di governo e il Ministro per la funzione pubblica si farà promotore di una iniziativa che prevede la realizzazione di uno strumento informativo di supporto delle amministrazioni per la supervisione e misurazione degli stati di avanzamento dei rispettivi programmi, rispetto agli obiettivi fissati nel piano di Governo. L'attivazione di tale strumento prevede la realizzazione e la diffusione di una soluzione informatica presso le diverse amministrazioni, che costituiranno i punti di rilevazione delle informazioni per la gestione del programma.
Acquisto di beni e servizi
Nel corso del 2002 la Consip - Concessionaria servizi informativi pubblici - S.p.a. avvierà la nuova piattaforma tecnologica di e-procurement, che consentirà di svolgere tutte le attività di acquisizione di beni e servizi per via elettronica.
Nel contempo il Dipartimento per l'innovazione e le tecnologie sta predisponendo il regolamento sul commercio elettronico e sulle aste on line, al fine di disciplinare la materia.
Il compito delle amministrazioni sarà quello di utilizzare il primo semestre del 2002 per avviare le misure organizzative e formative, che consentano di utilizzare il sistema di e-procurement nel momento in cui sarà disponibile.

Nel 2002 il Dipartimento per l'innovazione e le tecnologie studierà la possibilità di introdurre la carta di credito (procurement card) per i responsabili della funzione acquisti, al fine di aumentare la responsabilizzazione dell'acquisto, indicando chiari limiti per tipologia di voci di acquisto e per importi di spesa.

Gestione della contabilità finanziaria ed economica

Ogni amministrazione avvierà programmi per la progressiva eliminazione (2002/2003) della modalità di compilazione manuale di documenti di natura contabile. Ogni operazione di natura contabile (gestione degli stanziamenti, assestamenti, impegni, mandati di pagamento) dovrà essere effettuata per via elettronica. I documenti saranno approvati con firma elettronica.

Qualora l'amministrazione non utilizzi la Rete unitaria della pubblica amministrazione per il trasporto e per l'interoperabilità, essa dovrà garantirsi, con il proprio provider, le misure necessarie ad assicurare la certezza e la sicurezza della transazione.

Per attuare il controllo di gestione tutte le amministrazioni dovranno dotarsi entro il 2002 di sistemi informativi di gestione della contabilità finanziaria ed economica, che, oltre a garantire gli adempimenti contabili richiesti dalla normativa, costituiranno strumenti di controllo della performance e dell'efficienza delle strutture.

Gestione del personale

Nel corso del 2002 sarà avviata la realizzazione del nuovo Sistema unitario di amministrazione e gestione del personale. Il progetto attualmente in corso ha l'obiettivo da un lato di costruire un sistema direzionale di governo del personale in grado di gestire tutte le informazioni riguardanti i percorsi professionali e formativi, dall'altro di finalizzare la progressiva realizzazione di un sistema per il pagamento delle competenze del personale delle amministrazioni dello Stato. Ogni amministrazione dovrà partecipare alla revisione dei requisiti e alle attività di verifica che saranno svolte nella fase di avvio del nuovo sistema.

La realizzazione del sistema direzionale di governo del personale dovrà essere effettuata mettendo a fattor comune le esigenze delle diverse amministrazioni e favorendo lo scambio di know how ed il riuso di soluzioni già disponibili.

L'attività di elaborazione paghe e di pagamento delle competenze dovrà essere ottimizzata introducendo modalità operative che consentano lo scambio delle informazioni tra le amministrazioni per via elettronica (es. rilevazione di presenze, assenze e straordinari, determinazione delle competenze ordinarie ed accessorie).

Nel contempo dovrà essere avviato un sistema intranet, che contenga tutta la modulistica necessaria affinché il colloquio fra dipendente ed amministrazione avvenga anch'esso per via elettronica. Una volta avviata l'intranet non saranno più gestite operazioni per via cartacea.

Lo scambio di documenti fra il dipendente e le amministrazioni può prevedere il ricorso alla firma elettronica, nei casi in cui è necessario, in modo da garantire il dipendente sulla certezza dell'invio e della ricezione dei documenti. A tal fine ogni amministrazione distribuirà le firme elettroniche al propri dipendenti prima di avviare le nuove modalità di interazione con il personale.

Lo scambio di informazioni fra dipendente e pubblica amministrazione potrà avvenire eventualmente anche attraverso «call center» dedicati, che potranno essere comuni a più amministrazioni o attivati dalla singola amministrazione centrale.

Nel corso del 2002 l'amministrazione dovrà studiare il modo per ridisegnare i processi interni in modo da «digitalizzare completamente» il processo di gestione delle richieste presentate, rivedendo l'organizzazione del lavoro, le competenze, le responsabilità ed attivando le semplificazioni necessarie per il conseguimento in tempi rapidi del cambiamento.

3.3. Potenziare l'attuale infostruttura.

Il conseguimento, già nel corso del 2002, dei primi risultati sulle iniziative illustrate richiede il lancio di programmi di potenziamento dell'infostruttura, intendendo come tale l'insieme degli strumenti, delle norme e delle azioni strutturali che favoriscano l'utilizzo diffuso delle tecnologie ed il cambiamento nelle modalità operative di gestione della pubblica amministrazione.

Sicurezza

Al fine di garantire la sicurezza del patrimonio informativo dell'amministrazione, il Dipartimento per l'innovazione e le tecnologie e il Ministero delle comunicazioni, stanno predisponendo una specifica direttiva sulla sicurezza ICT.

Tale direttiva definisce un percorso che inizia con un'autovalutazione sul livello di sicurezza tecnologica di ogni amministrazione, per arrivare a definire il proprio livello di rischio.
Il 2002 sarà l'anno dell'allineamento delle amministrazioni a tale direttiva.
Postazione di lavoro informatizzata
Nel corso del 2002, al fine di rendere possibile l'avvio della «digitalizzazione della PA», sarà necessario dotare la maggior parte dei dipendenti delle pubbliche amministrazioni di una postazione di lavoro informatizzata. Il raggiungimento di tale obiettivo richiede il completamento della cablatura delle amministrazioni, in modo da consentire la totale interoperabilità.
Tutte le postazioni di lavoro dovranno essere in rete, disporre di collegamento a Internet, di una stampante di servizio (eventualmente una per più computer), del software di office automation in dotazione dell'amministrazione e, ove necessario, di scanner per gestire la documentazione che dovrà essere trasportata in rete e consultata.
La Consip renderà disponibili le convenzioni necessarie per facilitare l'acquisizione dell'hardware, in leasing o in «fleet management», per liberare l'amministrazione dalla gestione delle postazioni.
Carta multiservizi del dipendente
Un importante segnale di cambiamento nel rapporto fra dipendente e pubblica amministrazione sarà costituito dalla sostituzione, nel corso del 2002, della normale «tessera di plastica» distribuita ad ogni dipendente per il riconoscimento e quindi principalmente per scopi di sicurezza interna, con una carta a microcircuito che contenga la firma digitale.
La carta potrà essere adibita a diversi usi quali ad esempio: controllo accessi, identificazione personale, firma digitale, addebito, mensa, ecc.
Valorizzazione del patrimonio informativo esistente
Ad oggi esiste all'interno della pubblica amministrazione un vasto patrimonio informativo, spesso non adeguatamente conosciuto e sfruttato. Una maggiore conoscenza delle basi informative di proprietà dell'amministrazione può consentire notevoli risparmi e può facilitare l'avvio di una maggiore «cooperazione applicativa», consentendo una progressiva integrazione dell'intero sistema informativo pubblico.
Nel corso del 2002 le varie amministrazioni, sulla base delle proprie basi di dati, forniranno al Dipartimento per l'innovazione e le tecnologie un'adeguata informativa sulle proprie banche dati, proponendo anche diverse possibilità di utilizzo e possibili integrazioni.
Questa attività potrebbe riguardare alcune importanti banche dati ad oggi non «condivise» o in corso di realizzazione. Si pensi, ad esempio, alla banca dati sugli investimenti pubblici, alle anagrafi o al catasto.
Il Dipartimento per l'innovazione e le tecnologie, di concerto con le altre amministrazioni, predisporrà nel 2002 i piani e le necessarie condizioni affinché, già nel 2003, si attivino le prime applicazioni cooperative tra le amministrazioni.
La condivisione del patrimonio informativo disponibile e delle esperienze condotte nelle amministrazioni consentirà l'individuazione di strumenti di eccellenza per la gestione delle banche dati, favorendone la diffusione ed il riuso.
3.4. Sviluppare le competenze informatiche e tecnologiche dei dipendenti dello Stato.
Il Dipartimento per l'innovazione e le tecnologie e il Dipartimento della funzione pubblica, nell'àmbito di un più ampio progetto di change management e formazione, avvierà concrete iniziative per il completamento dell'alfabetizzazione informatica di tutti i dipendenti della pubblica amministrazione e per l'apprendimento della lingua inglese e dell'utilizzo di Internet.
I corsi avranno l'obiettivo di spingere l'avvio del processo di digitalizzazione, garantendo un progressivo allineamento delle competenze dei manager pubblici a quelle del settore privato, in particolare in termini di conoscenza delle tecnologie più avanzate.
Il Dipartimento per l'innovazione e le tecnologie e il Dipartimento della funzione pubblica definiranno entro marzo 2002 i programmi dei corsi, i sistemi di valutazione, i sistemi di incentivazione e premianti legati alla diffusione della cultura tecnologica nella pubblica amministrazione.
e-learning
La diffuisione di tecniche di formazione a distanza favorisce l'affermazione della cultura tecnologica nella pubblica amministrazione e fornisce un supporto alla crescita delle competenze professionali dei dipendenti.

I programmi di formazione sull'Information and Communication Technology possono fare leva sulle opportunità offerte dall'e-learning, consentendo una alfabetizzazione informatica omogenea e coordinata all'interno della pubblica amministrazione.
3.5. Promuovere la diffusione dell'innovazione nel Paese.
Iniziativa Larga Banda.
Il 2002 sarà l'anno dell'avvio di alcune grandi iniziative che avranno un impatto significativo sui cittadini e sulle imprese.
Un'iniziativa prioritaria, avviata dal Ministro per l'innovazione e le tecnologie e dal Ministro delle comunicazioni, è quella finalizzata alla diffusione ed allo sviluppo della Larga Banda nel Paese.
La commissione di studio, nominata dal Ministro per l'innovazione e le tecnologie e dal Ministro delle comunicazioni, ha confermato che la diffusione della Larga Banda nel Paese può essere una leva importante per lo sviluppo della Società dell'informazione.
La pubblica amministrazione rappresenta un punto di riferimento importante per la diffusione della Larga Banda, sia per la sua capacità di attivare il settore privato, sia per la capacità di avviare programmi concreti, che prevedano il ricorso all'utilizzo di banda.
In particolare, il compito del Dipartimento per l'innovazione e le tecnologie sarà quello di aggregare la domanda pubblica di Larga Banda attraverso l'adozione di modelli di approvvigionamento quali la centrale acquisti. Il consolidamento di una massa critica di acquisto consentirebbe, inoltre, di generare significative economie di scala.
Servizi digitali su Larga Banda.
La diffusione della Larga Banda si configura quale fattore cruciale per lo sviluppo di servizi digitali ai cittadini ed alle imprese.
Tra questi, l'e-learning rappresenta una opportunità ad elevato potenziale, in particolare in alcune aree critiche della pubblica amministrazione.
Nel mondo della sanità può essere applicata, ad esempio ai programmi di formazione dei medici di base al fine di migliorare la qualità del servizio sanitario nazionale ed il livello di soddisfazione dei cittadini.
Può essere applicata inoltre ai servizi di telemedicina che rappresentano una delle applicazioni più avanzate in campo sanitario.
Pertanto nel 2002 il Ministero della salute in collaborazione con il Dipartimento per l'innovazione e le tecnologie, avvieranno programmi pilota sull'utilizzo della Larga Banda.
Altra area chiave è quella della scuola, dove l'utilizzo di infrastrutture a Larga Banda potrà consentire l'integrazione degli strumenti e delle modalità didattiche tradizionali con applicazioni digitali caratterizzate da un elevato grado di interattività e di multimedialità.
L'utilizzo dell'infrastruttura a Larga Banda potrà, inoltre, essere un veicolo per attuare un piano di informatizzazione dei programmi di aggiornamento professionale degli insegnanti.
Altre aree di evidente interesse da approfondire nel corso del 2002 sono il telelavoro e la fruizione dei beni culturali (musei digitali).
3.6. Strumenti innovativi di coordinamento e gestione delle iniziative.
L'obiettivo di conseguire un rapido, visibile e misurabile sviluppo dell'innovazione nella pubblica amministrazione richiede l'adozione di strumenti di gestione dei programmi, capaci di garantire il coordinamento degli interventi e di renderne possibile il controllo ed il monitoraggio.
Alla luce di tale premessa è opportuno attivare metodologie di lavoro che prevedano:
una azione concertata tra le diverse amministrazioni;
una azione sinergica ed unitaria del Dipartimento per l'innovazione e le tecnologie, del Dipartimento della funzione pubblica e del Ministero delle comunicazioni nella gestione dell'intero processo di digitalizzazione della pubblica amministrazione statale.
Il coordinamento delle singole iniziative previste nella presente direttiva ed il monitoraggio sistematico dei risultati conseguiti, saranno garantiti dall'avvio di un processo orientato al lavoro di gruppo e basato sull'apertura di tavoli di lavoro permanenti, cui parteciperanno il Dipartimento per l'innovazione e le tecnologie ed i «Referenti», opportunamente identificati dalle singole amministrazioni statali.
I piani di attuazione della presente direttiva relativi a ciascuna amministrazione saranno predisposti, nel corso del mese di gennaio 2002, dai «Referenti» e successivamente condivisi nell'àmbito di tavoli permanenti di lavoro fra il Dipartimento per l'innovazione e le tecnologie ed i Referenti stessi.

L'attuazione dei piani di intervento predisposti prevede l'intervento dei Servizi di Controllo Interno, previsti presso ciascuna amministrazione e deputati alla diffusione di meccanismi di pianificazione e controllo nelle strutture amministrative di propria competenza.
I servizi di controllo interno contribuiranno al monitoraggio ed all'attuazione degli indirizzi formulati nell'àmbito dei piani di intervento, anche al fine di individuare le migliori prassi interne alle amministrazioni e di favorire il riuso e la diffusione delle metodologie e degli strumenti che le supportano.
Per quanto attiene all'immediato recepimento della presente direttiva, il Dipartimento per l'innovazione e le tecnologie assicurerà la necessaria consulenza ed assistenza al fine di agevolare le relative strutture nella predisposizione e nella attuazione delle direttive di competenza.
Sarà comunque necessario far pervenire tempestivamente anche al Dipartimento per l'innovazione e le tecnologie gli schemi delle direttive di ciascun Ministro.
4. Azioni ed indicatori di misurazione.
Al fine di giungere ad una definizione coordinata ed esaustiva dei piani di attuazione della presente direttiva, si propone di seguito un quadro riepilogativo delle principali azioni che si dovranno prevedere in risposta alle priorità di intervento identificate ed una lista di indicatori di riferimento con i quali misurare i risultati conseguiti nel 2002.
Quelle indicate si configurano quali azioni prioritarie e rappresentano il minimo di interventi da avviare nel 2002, ad integrazione e complemento dei piani predisposti autonomamente dalle singole amministrazioni.
Gli indicatori proposti rappresentano il principale strumento di monitoraggio dello stato di avanzamento del processo di innovazione. Il flusso di ritorno del monitoraggio verrà indirizzato al Dipartimento per l'innovazione e le tecnologie che potrà cosi disporre di un quadro complessivo del grado di raggiungimento degli obiettivi prioritari indicati.
4.1. Indicatori proposti per obiettivo.
Migliorare il livello di servizio
Azione 1: attivazione di Uffici digitali per il cittadino
Indicatore: numero di Uffici digitali avviati per amministrazione
Azione 2: realizzazione portale nazionale del cittadino (e-Italia)
Indicatore: numero di servizi digitali erogati dal portale per amministrazione
Favorire l'efficienza e l'economicità di gestione
Azione 1: rilascio nuova piattaforma e-procurement
Indicatore: percentuale di acquisti effettuati on line
Azione 2: semplificazione delle attività di natura contabile
Indicatori: percentuale di mandati di pagamento elettronici, di firme elettroniche distribuite nella pubblica amministrazione, di flussi gestiti con protocollo informatico
Azione 3: realizzazione del nuovo Sistema Informativo Unitario del Personale
Indicatore: percentuale di uffici di servizio collegati al Sistema Informativo Unitario del Personale
Azione 4: sistemi di comunicazione multicanale (intranet e call-center) per i dipendenti pubblici
Indicatore: grado di saturazione dell'intranet e del call-center (utilizzo/capacità)
Azione 5: Sviluppo protocollo e flussi documentali
Indicatore: percentuale di aree organizzative omogenee in cui il nucleo minimo è operante
Potenziare l'attuale infostruttura
Azione 1: interventi sulla sicurezza delle informazioni in formato digitale
Indicatore: allineamento alla direttiva sulla sicurezza in corso di emanazione
Azione 2: informatizzazione delle postazioni di lavoro (infrastruttura di rete, hardware e software)
Indicatore: percentuale postazioni di lavoro informatizzate rispetto al numero dei dipendenti
Azione 3: lancio carta multiservizi per i dipendenti pubblici
Indicatore: numero carte emesse
Azione 4: valorizzazione patrimonio informativo disponibile
Indicatore: numero di banche dati messe in condivisione
Sviluppare le competenze informatiche e tecnologiche dei dipendenti dello Stato
Azione 1: alfabetizzazione informatica
Indicatore: ore di formazione ICT erogate
Azione 2: introduzione metodologie di e-learning

Indicatore: ore di formazione a distanza erogate
Promuovere la diffusione dell'innovazione nel paese
Azione 1: sviluppo della «larga banda»
Indicatore: numero di connessioni Larga Banda attivate
Azione 2: sviluppo servizi digitali su Larga Banda
Indicatore: numero di servizi digitali su Larga Banda

CAPITOLO II

PROGETTI DI E-GOVERNMENT

La I^ fase di attuazione dell'e-government nelle Regioni e negli Enti Locali si è sviluppata tra ottobre 2001 ed aprile 2003, secondo tre linee di azione fortemente correlate fra loro: la promozione di progetti di e-government volti allo sviluppo di servizi infrastrutturali e servizi finali all'utenza, la definizione di un comune quadro tecnico e metodologico di riferimento, la creazione della rete dei Centri Regionali di Competenza (CRC). La prima linea di azione si è realizzata mediante l'emissione di un Avviso per il cofinanziamento di progetti finalizzati all'individuazione e realizzazione di servizi on-line per cittadini ed imprese. La valutazione dei progetti ha messo in luce il buon livello di progettualità espressa dal territorio, che ha consentito di selezionare 134 progetti, di cui 26 nel Sud, per complessivi 500 milioni di euro (di cui 120 ml cofinanziati dal Ministero per l'innovazione e le tecnoclogie). I progetti selezionati sono finalizzati in massima parte all'erogazione di servizi pubblici in rete a larga parte della popolazione e delle imprese. Gli obiettivi che tali progetti si propongono riguardano da un lato la semplificazione, l'efficienza e la competitività delle circa 4.000 pubbliche amministrazioni che si sono impegnate in questo percorso di modernizzazione; dall'altro il sostegno alla coerenza ed integrazione tra il livello locale e il sistema nazionale. Coerentemente agli obiettivi illustrati, l'ICT è utilizzata dai progetti quale risorsa strategica per la definizione del rapporto tra le diverse autonomie locali e l'armonizzazione dei processi innovativi a livello nazionale. Nella primavera del 2003 sono state firmate tutte le convenzioni di attivazione dei progetti. Da giugno 2003 a marzo 2004 il CNIPA (Centro nazionale per l'informatica nella pubblica amministrazione) è all'indirizzo ha supportato la pianificazione esecutiva dei progetti cofinanziati, propedeutica all'avvio del monitoraggio dello stato avanzamento dei lavori. Il sistema di monitoraggio applicato rappresenta un approccio innovativo finalizzato alla puntuale verifica delle attività progettuali effettivamente realizzate ed alla conseguente erogazione delle diverse tranche di cofinanziamento previste.

La II^ fase si differenzia per il fatto di non prevedere un unico bando nazionale, ma diverse azioni mirate. Essa prevede la realizzazione di cinque linee di azione:

1. *Lo sviluppo dei servizi infrastrutturali locali e Sistema Pubblico di connettività (SPC)*
2. *Diffusione territoriale dei servizi per cittadini ed imprese (riuso)*
3. *L'inclusione dei piccoli Comuni nell'attuazione dell' e-government*
4. *L'avviamento di progetti per lo sviluppo della cittadinanza digitale (e-democracy)*
5. *La promozione dell'utilizzo dei nuovi servizi presso cittadini e imprese*

Linea 1. Lo sviluppo dei servizi infrastrutturali locali e SPC

Obiettivo: individuare e cofinanziare progetti finalizzati alla realizzazione di servizi infrastutturali adeguati per l'erogazione di servizi finali: i servizi delle reti regionali e/o territoriali e le strutture per la loro gestione, i servizi di gestione delle carte dei servizi a livello regionale, i servizi di interoperabilità dei protocolli e della gestione documentale.

Le Amministrazioni pubbliche centrali e locali saranno sempre più interconnesse per semplificare i rapporti fra i cittadini e la pubblica amministrazione. Sono 56 infatti i progetti regionali cofinanziati dal CNIPA. Prende il via un articolato programma di investimenti per quasi 100 ml, di cui 35 in co-finanziamento, per creare infrastrutture di rete che consentano ai cittadini e alle imprese di accedere in modo rapido e sicuro ai servizi di e-government. In particolare i 56 progetti ammessi al co-finanziamento statale, pari al 97% di quelli presentati, puntano a creare le condizioni per condividere il patrimonio informativo tra enti e permettere una gestione delle pratiche e dei procedimenti più veloce e sicura. In tal modo tutte le PA potranno accedere a banche dati comuni e archivi condivisi, grazie all'integrazione delle applicazioni informatiche. Le proposte sono finalizzate allo sviluppo, al potenziamento e alla gestione di reti regionali e territoriali; i servizi di gestione delle Carte Servizi regionale; i servizi per l'interoperabilità e la cooperazione applicativa; il protocollo informatico e i servizi per la gestione documentale.

Linea 2. Diffusione territoriale dei servizi per cittadini ed imprese (riuso)

Non si ritiene conveniente, nella seconda fase di attuazione, promuovere la realizzazione di nuovi progetti di e-government mediante nuovi bandi. I progetti di e-gov attualmente cofinanziati prevedono infatti la realizzazione di tutti i servizi prioritari che erano stati indicati come riferimento. La realizzazione in corso però non coinvolge tutte le amministrazioni in modo omogeneo, e non include molti piccoli e medi comuni. La linea di azione ha come obiettivo l'allargamento alla maggior parte delle amministrazioni locali dei servizi per cittadini e imprese in corso di realizzazione con i progetti di e-government (riuso). L'attuazione di questo processo prevede la creazione di un catalogo delle soluzioni di e-gov, basato sulle "offerte" pervenute in risposta all'avviso e la presentazioni di progetti di riuso, in risposta ad un secondo avviso. In risposta al 1° avviso sono pervenute al Cnipa da parte dei coordinatori di 84 progetti cofinanziati nell'ambito del 1° avviso, 270 soluzioni offerte al riuso, per le quali è stato richiesto l'inserimento a catalogo.

Sono 84 i progetti cofinanziati dal 1° avviso di e-gov ad aver presentato soluzioni per il Catalogo. In totale 270 soluzioni a disposizione delle amministrazioni che non hanno partecipato alla prima fase e che potranno avvalersi di strumenti di innovazione già collaudati. Il valore autentico non è nel semplice riutilizzo del software, bensì l'acquisizione di un ricco insieme di competenze progettuali e di esperienze pratiche. Il catalogo sarà ordinato in "aree tematiche": ognuna di esse sarà corredata di informazioni anagrafiche (progetto di origine, amministrazione di appartenenza, tipologia, servizi erogati) e di un documento analitico. Contestualmente all'uscita del catalogo è pubblicato l'avviso che consente agli enti di scegliere tra le soluzioni presenti disponibili e di presentare un vero e proprio "progetto di riuso", valutato da una commissione ad hoc che deciderà su un eventuale cofinanziamento.

<u>Linea 3. L'inclusione dei comuni piccoli nell'attuazione dell' e-government</u>

La linea di azione ha come obbiettivo l'avvio di esplicite attività di sostegno verso i piccoli comuni, per garantirne la partecipazione piena ai processi di innovazione dell' e-government. I comuni con meno di 5000 abitanti ("piccoli comuni") sono oggi 5.836, ed in essi risiedono più di 10 milioni di abitanti. La linea di azione si pone come fine di sostenere i processi di associazionismo e di cooperazione tra i piccoli Comuni, favorire

economie di gestione con particolare riferimento alla spesa ICT, migliorare la qualità dei servizi offerti a cittadini, imprese e territorio, attivare iniziative per la riduzione del divario digitale sul territorio.

Linea 4. L'avviamento di progetti per lo sviluppo della cittadinanza digitale (e-democracy)

Obiettivo: avviare progetti di utilizzo delle tecnologie ICT come strumento per promuovere la partecipazione dei cittadini alla vita delle amministrazioni pubbliche e alle loro decisioni. I progetti devono quindi prevedere l'utilizzo di tecnologie adeguate in termini di affidabilità ed accessibilità, la promozione della partecipazione attiva dei cittadini, la garanzia del coinvolgimento effettivo dei decisori pubblici, la valutazione dei risultati del processo di partecipazione.

La Commissione di valutazione ha ammesso al cofinanziamento 57 dei 129 progetti presentati al CNIPA in risposta all'"Avviso per la promozione della cittadinanza digitale" (e-democracy) per un per un totale di 9,5 Ml di cofinanziamento, a fronte di un importo complessivo di spesa pari a 41 Ml. Fra questi vi è anche il progetto denominato «Sesamo: la porta è aperta - Accesso al Palazzo Virtuale delle Pubbliche Amministrazioni», promosso dal Consiglio regionale del Piemonte, d'intesa con le Regioni Liguria, Valle d'Aosta e le Province piemontesi.

Tale progetto che ha anche avuto un'ottima valutazione, considerando che ha ottenuto 71,5 punti, mentre il punteggio massimo è stato di 88,5 e quello minimo di11,5, si pone l'obiettivo di favorire lo sviluppo della comunicazione digitale tra cittadini e istituzioni, sia aiutando le aree territoriali non facilmente raggiunte da servizi telematici, sia intervenendo per avvicinare all'informatica le categorie di utenti svantaggiate per cultura o per diversa abilità fisica. ed

Le tematiche affrontate dai progetti di e-democracy riguardano essenzialmente ambiente e territorio, interventi sociali e urbanistica, tributi, tasse locali e sanità. 11 progetti si sono concentrati su di una unica politica locale, molti hanno deciso di implementare più politiche, 12 progetti affrontano invece più di 10 politiche locali. Fra gli enti finanziati, i comuni sotto i 5.000 abitanti rappresentano la metà degli enti ammessi

al finanziamento. Ben l'85% dei progetti finanziati coinvolgono Associazioni rappresentative della società civile, con la partecipazione di 450 fra associazioni di categoria, onlus, ong, circoli, etc. In particolare, l'attenzione dei progetti si concentra sui processi di decisione pubblica, con l'obiettivo di migliorarne l'efficacia, l'efficienza e la condivisione con tutti gli attori coinvolti. L'e-democracy rappresenta, all'interno della II. fase del piano di e-gov, una linea di azione con una forte propensione sperimentale. Un'azione caratterizzata da una forte innovatività e originalità – sia in termini di contenuti che di approccio alle tecnologie – con l'obiettivo di favorire e incentivare dinamiche di adozione e sperimentazione da parte delle Regioni e delle Amministrazioni locali.

Linea 5. La promozione dell'utilizzo dei nuovi servizi presso cittadini e imprese

La linea di azione ha come obiettivo la promozione dell'uso dei nuovi servizi presso cittadini e imprese. La realizzazione di servizi on-line è condizione necessaria, ma non sufficiente per l'utilizzo degli stessi. E' necessario infatti spostare fasce consistenti di utenza dalla fruizione tradizionale dei servizi alla fruizione dei servizi mediante le nuove modalità di erogazione. A tale scopo ogni amministrazione dovrà prevedere sul proprio territorio un' efficace azione di comunicazione verso la propria utenza.. Tali attività di comunicazione faranno riferimento a formati, strumenti e risorse di comunicazione definite per l'insieme dei progetti di e-government, con l'obiettivo di comunicare non solo la disponibilità di un nuovo servizio, ma l'attuazione di un vasto programma di innovazione realizzato congiuntamente da tutte le amministrazioni.

Pubblicato in Gazzetta Ufficiale l'avviso per la selezione di progetti e-learning.

NUMERO SCHEDA: 6434

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: GAZZETTA UFFICIALE

NUMERO: 160

DATA: 12/07/2005

NATURA ATTO: COMUNICAZIONE

Sulla Gazzetta Ufficiale n. 160 del del 12 luglio 2005 è stato pubblicato il comunicato del CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione), contenente l'avviso per la selezione di progetti e-learning. L'avviso ha lo scopo di individuare e cofinanziare progetti - proposti dalle Regioni e dalle Province Autonome di Trento e Bolzano ("enti proponenti") - che abbiano come fine la promozione dell'utilizzo delle metodologie e tecnologie di e-learning per la formazione dei propri dipendenti e di quelli degli enti locali del proprio territorio. I progetti potranno essere presentati dalle amministrazioni proponenti scegliendo tra i 5 temi indicati nell'Avviso:

1. Management e utilizzazione dei sistemi informativi (EUCIP);
2. La gestione dei flussi documentali e le nuove modalità lavorative;
3. Il Project finance: come progettare l'innovazione utilizzando finanziamenti per le pubbliche amministrazioni ;
4. Sicurezza e Privacy delle informazioni e dei dati nei sistemi informativi;
5. La gestione per l'acquisizione di beni e forniture di servizi (gestione di bandi e gare per progetti di innovazione tecnologica).

Il cofinanziamento assegnato ai singoli progetti non potrà superare il 40% del costo del progetto, con un tetto massimo di cofinanziamento di 400.000,00. La gestione dell'Avviso avverrà secondo le modalità già collaudate per i progetti e-government. Per eventuali chiarimenti sul testo dell'avviso è stato istituito un servizio di help desk: scuola-virtuale@cnipa.it.

Si riporta il testo del comunicato.

CENTRO NAZIONALE PER L'INFORMATICA NELLA PUBBLICA AMMINISTRAZIONE
COMUNICATO
Art. 1.
Obiettivi

1. Nell'ambito dell'attuazione del piano di e-Government, il presente avviso ha lo scopo di individuare e cofinanziare progetti, proposti dalle regioni e dalle province autonome di Trento e Bolzano (di

seguito indicati «enti proponenti»), finalizzati alla promozione dell'utilizzo delle metodologie e delle tecnologie di e-learning per la formazione dei propri dipendenti e di quelli degli enti locali presenti sul proprio territorio. 2. Il Centro nazionale per l'informatica nella pubblica amministrazione - CNIPA cofinanziera' i progetti individuati, fino all'importo complessivo di Euro 2.000.000,00.

Art. 2.

Ambito di intervento dei progetti

1. Il presente avviso riguarda la progettazione, lo sviluppo, la realizzazione, il monitoraggio, la valutazione (controllo) di iniziative progettuali attinenti ad attivita' formative.

2. Le attivita' formative dovranno essere rivolte ai dirigenti ed ai funzionari responsabili di servizio degli enti proponenti e degli enti locali presenti sul proprio territorio.

3. I progetti presentati dovranno sviluppare uno o piu' dei seguenti temi: a) management e utilizzazione dei sistemi informativi (EUCIP); b) gestione dei flussi documentali e nuove modalita' di lavoro; c) project finance: come progettare l'innovazione utilizzando finanziamenti per le pubbliche amministrazioni; d) sicurezza e privacy delle informazioni e dei dati nei sistemi informativi; e) acquisizione di beni e forniture di servizi (adempimenti connessi alla predisposizione di bandi e alla realizzazione di gare per progetti di innovazione tecnologica).

4. Le proposte progettuali dovranno essere conformi a quanto previsto: dalla direttiva 6 agosto 2004 del Ministro per l'innovazione e le tecnologie e del Ministro per la funzione pubblica, recante: «Progetti formativi in modalita' e-learning nelle pubbliche amministrazioni"», indicata nelle premesse; dalle linee guida per i progetti formativi in modalita' e-learning nelle pubbliche amministrazioni; dal Vademecum per la realizzazione di progetti formativi in modalita' e-learning nelle pubbliche amministrazioni. 5. I progetti dovranno, inoltre, essere coerenti con i piani formativi degli enti proponenti. 6. Il completamento dei progetti cofinanziati dovra' avvenire entro 18 mesi dalla data di perfezionamento della convenzione di cui al successivo art. 5.

Art. 3.

Soggetti ammessi

1. I soggetti beneficiari del cofinanziamento ed aventi titolo a presentare i progetti come sopra individuati sono le regioni e le province autonome di Trento e Bolzano. 2. I destinatari di ciascun progetto di e-learning saranno i dirigenti ed i funzionari responsabili di un servizio degli enti proponenti e, in misura non inferiore al 50%, dei rispettivi enti locali: province, comuni, unioni di comuni, comunita' montane, comunita' isolane e di arcipelago. 3. Gli enti locali individuati al comma precedente dovranno sottoscrivere un accordo con l'ente proponente il progetto. Tale accordo, stipulato tramite protocollo d'intesa, dovra' essere allegato ai documenti di progetto per la partecipazione al cofinanziamento di cui al presente avviso.

Art. 4.

Ammissibilita' dei progetti

1. I progetti sono ritenuti ammissibili se: a) presentati da uno dei soggetti indicati al precedente art. 3, comma 1; b) compilati sull'apposita modulistica elettronica predisposta dal CNIPA e resa disponibile agli indirizzi indicati al successivo art. 10; c) presentati entro, e non oltre, la data di scadenza indicata all'art. 6, comma 3, secondo le modalita' specificate nella «Guida alla presentazione dei progetti».

Art. 5.

Cofinanziamenti

1. Il cofinanziamento assegnato ai singoli progetti di cui al presente avviso non potra' superare il 40% del costo totale degli stessi, con un tetto massimo di Euro 400.000,00; resta a carico dei soggetti proponenti la copertura della quota residua. 2. Nel caso in cui un progetto benefici di ulteriori finanziamenti, il cofinanziamento erogato dal CNIPA, sommato agli altri, sara' di entita' tale da non determinare un finanziamento totale, per ogni progetto, superiore ai costi stimati di ciascun progetto medesimo. 3. I rapporti tra il CNIPA e gli enti assegnatari dei cofinanziamenti sono regolati da apposita convenzione, il cui schema sara' reso disponibile agli indirizzi di cui al successivo art. 10. 4. Il cofinanziamento sara' erogato in quattro tranche cosi' individuate: il 20%, successivamente alla stipula della convenzione con il CNIPA di cui al comma precedente ed alla formalizzazione dell'aggregazione di cui all'art. 3, comma 3; il 30%, successivamente alla positiva valutazione, da parte di un Comitato tecnico nominato dal CNIPA, della progettazione esecutiva dell'intervento formativo e alla

produzione di tutti i materiali didattici previsti dal progetto; un ulteriore 30% successivamente alla positiva valutazione, da parte del suddetto Comitato, dei risultati della fruizione da parte di almeno il 50% dei destinatari del progetto; il restante 20%, successivamente alla conclusione del progetto ed alla positiva valutazione, effettuata dal suddetto Comitato tecnico, del raggiungimento degli obiettivi previsti dal progetto medesimo.

Art. 6.

Presentazione dei progetti

1. La trasmissione delle proposte di progetto e la documentazione attestante la formalizzazione dell'aggregazione dovranno avvenire esclusivamente in formato elettronico, secondo le modalita' indicate nell'allegato «Guida alla presentazione dei progetti», disponibile agli indirizzi indicati al successivo art. 10. 2. I progetti dovranno essere firmati digitalmente dal legale rappresentante dell'ente proponente, o da un suo delegato, secondo le modalita' indicate nell'allegato «Guida alla presentazione dei progetti"». 3. Le proposte di progetto dovranno pervenire all'indirizzo di posta elettronica elearning@cnipa.it entro, e non oltre, 90 giorni dalla data di pubblicazione del presente avviso nella Gazzetta Ufficiale della Repubblica italiana

Art. 7.

Valutazione dei progetti

1. I progetti saranno valutati dall'apposita commissione prevista all'art. 3, comma 4, del citato decreto del Presidente del Consiglio dei Ministri 14 febbraio 2002, che proporra' al CNIPA la relativa graduatoria, l'assegnazione dei finanziamenti e l'ammontare di ciascuno. 2. I progetti saranno valutati sulla base dei criteri di seguito descritti (riportati in ordine decrescente d'importanza): *(omissis)*

Art. 8.

Monitoraggio

1. CNIPA effettuera' il controllo dello stato di avanzamento dei progetti sulla base di un apposito piano presentato dai proponenti i progetti stessi, con specifico riferimento a quanto prescritto dagli stati di avanzamento, come previsto al precedente art. 5, comma 4.

Art. 9.

Riuso dei progetti

1. Le amministrazioni beneficiarie dei cofinanziamenti si impegnano a mettere a disposizione delle altre amministrazioni pubbliche le esperienze e le soluzioni realizzate nell'ambito dei progetti cofinanziati sulla base di specifici accordi e nel rispetto della normativa vigente.

Art. 10.

Documenti e informazioni

1. La modulistica - con la relativa guida alla compilazione - la guida alla presentazione dei progetti, la direttiva del Ministro per l'innovazione e le tecnologie e del Ministro per la funzione pubblica 6 agosto 2004, recante: «Progetti formativi in modalita' e-learning nelle pubbliche amministrazioni - le Linee guida e il Vademecum per i progetti formativi in modalita' e-learning nelle pubbliche amministrazioni, i documenti di riferimento e qualunque altra informazione relativa al presente avviso sono disponibili ai seguenti indirizzi: a) http://www.cnipa.gov.it; b) http://www.crcitalia.it. 2. Per fornire eventuali chiarimenti sul testo dell'avviso e dei sopra richiamati documenti e' istituito un servizio di help desk, che opera esclusivamente per via telematica all'indirizzo scuola-virtuale@cnipa.it (tel. 0685264381)

Sono Stati creati i Centri regionali di competenza nell'ambito della strategia di cooperazione tra i livelli di governo coinvolti nell'e.government.

NUMERO SCHEDA: 4637

CLASSIFICAZIONE: E-GOVERNMENT

FONTE: IL SOLE 24 ORE

DATA: 30/04/2004

PAGINA: 7

NATURA ATTO: COMMENTO

Il Dipartimento per l'innovazione e le Tecnologie, d'intesa con il Dipartimento della Funzione Pubblica e con il supporto operativo del Formez, ha realizzato il progetto Centri Regionali di competenza per l'e-government e la Società dell'Informazione.In particolare, ciascun CRC è costituito sulla base di apposite convenzioni tra il Ministro per l'innovazione e le Tecnologie e i presidenti delle Regioni.
Il CRC è una struttura composta da operatori dei diversi livelli del governo regionale e locale che ha la finalità di affiancare e facilitare l'azione delle Autonomie Locali tesa ad innovare i servizi ed a sviluppare i piani e i progetti di e-government.
Si tratta di strutture snelle ed operative ubicate sul territorio regionale che hanno il ruolo di facilitare l'attuazione dei processi di innovazione attraverso la realizzazione di piani di attività formative, informative e di assistenza agli Enti Locali.
Ciascun centro sviluppa un piano di attività con modalità operative e finalità proprie, adeguate alle esigenze della realtà locale, e, al tempo stesso, è in rete con gli altri centri regionali e beneficia di servizi e supporti comuni.
Gli obiettivi del progetto si possono sintetizzare nel seguente modo:

- sviluppare la cooperazione tra il Dipartimento per l'Innovazione e le Tecnologie e i sistemi regionali, mettendo in rete i CRC in un network nazionale, rappresentativo del nuovo assetto istituzionale federalista e supportando la Commissione Permanente sull'Innovazione e le Tecnologie;
- supportare gli Enti Locali e rafforzarne le competenze nella definizione ed attuazione di programmi e progetti per l'e-government e la Società dell'Informazione, in coerenza con gli obiettivi fissati dalle Linee Guida del governo;
- definire e diffondere modelli, approcci e strumenti condivisi e integrati sugli aspetti critici della realizzazione dei processi di innovazione;
- sviluppare la cooperazione ed il coordinamento tra diversi livelli di governo nei sistemi regionali e favorire scambi e azioni comuni su scala interregionale.

I Centri attivi sono 20 (Liguria, Calabria, Emilia Romagna, Friuli - Venezia Giulia, Sicilia, Basilicata, Marche, Puglia, Toscana, Veneto, Umbria, Sardegna, Lombardia, Campania, Abruzzo, Piemonte, Valle d'Aosta, Provincia Autonoma di Trento, Provincia Autonoma di Bolzano e Lazio).
Contesto, motivazioni e obiettivi dell'intervento per la creazione dei Centri Regionali di Competenza sono contenuti nel "Progetto per una rete di Centri Regionali di Competenza per l'e-government nelle regioni italiane".

Le Regioni del centro-nord (in particolare Lombardia, Emilia, Toscana e Piemonte) tra le più attive nel campo dell'e-governament.

NUMERO SCHEDA: 3239

CLASSIFICAZIONE: E-GOVERNMENT

FONTE: ITALIA OGGI

DATA: 20/06/2003

PAGINA: 39-40

SCHEDE COLLEGATE: 1992

Notevoli sono i progressi che negli ultimi anni ha conosciuto l'e-governament, volto a migliorare i rapporti fra p.a. e cittadini e a favorire un dialogo elettronico fra i soggetti coinvolti.
In Italia sono già stati avviati tutti i 138 progetti co-finanziati dal Dipartimento per l'innovazione e le tecnologie (Dit) con il primo avviso. Dei 120 milioni di euro già stanziati (altri 120 saranno messi a disposizione entro la fine dell'anno), 80 sono stati destinati ai 98 progetti che attuano servizi ai cittadini e alle imprese e 40 alle 40 iniziative per la realizzazione di infrastrutture telematiche a livello territoriale.
Tra i progetti attivati, servizi fiscali e catastali tramite internet e acquisto di forniture on-line con l'e-procurement.
Le Regioni del centro-nord risultano le più attive nel dare impulso allo sviluppo dell'e-governament: tra queste, spiccano la Lombardia – la regione che ha investito le maggiori risorse in questo campo (il piano d'azione e-Lomb@ardia ha un valore complessivo di oltre 800 milioni di euro e già 107 sono i progetti attualmente operativi) -, l'Emilia Romagna (il programma di investimenti prevede una spesa di circa 120 milioni di euro per la realizzazione di 9 progetti e ulteriori 180 microprogetti), la Toscana (i mezzi finanziari per l'attuazione del piano regionale di e-governamente nel triennio 2003-2005 ammontano a circa 53 milioni di euro e 19 sono i progetti già attivati) e il Piemonte (con 50 milioni di euro spesi negli ultimi 5 anni per la realizzazione della infrastrutture informatico-telematiche; dei 9 progetti di e-governament presentati per il co-finanziamento, 6 sono quelli selezionati ma la Regione si è impegnata a finanziare autonomamente gli altri 3).

Relazione europea sull'attuazione del piano di e-europe.

NUMERO SCHEDA: 2392

CLASSIFICAZIONE: E-GOVERNMENT

NATURA ATTO: RELAZIONE

DATA ATTO: 12/02/2003

ORGANO: COMMISSIONE DELLA COMUNITA EUROPEA

Secondo la relazione definitiva eEurope 2002, adottata il 12 febbraio 2003 dalla Commissione europea, il Piano d'azione eEurope 2002, varato dal Consiglio europeo di Feira nel giugno 2000 con l'obiettivo di portare l'Europa on-line il più rapidamente possibile, ha dato risultati molto positivi. In particolare, si legge sul sito istituzionale del governo italiano, la connettività Internet è cresciuta rapidamente. Nel 2002, più del 90% delle scuole e delle aziende erano su Internet, più della metà degli europei erano utenti regolari e oggi il 43% delle famiglie europee sono on-line. Attualmente, l'Europa dispone della rete dorsale per la ricerca più veloce del mondo (GEANT). La prossima sfida sarà la diffusione dei collegamenti ad alta velocità presso le famiglie e le PMI.
È stato adottato un quadro legislativo per le comunicazioni elettroniche e per il commercio elettronico, che entrerà in vigore quest'estate. I prezzi delle telecomunicazioni sono diminuiti; la concorrenza è aumentata e continuerà ad intensificarsi. Per il commercio elettronico, è stata adottata una serie di direttive per migliorare la certezza delle transazioni elettroniche, in particolare per quanto riguarda il commercio transfrontaliero, e garantire un livello adeguato di tutela dei consumatori.
Aumentare l'uso efficace di Internet è l'obiettivo della prossima fase, denominata eEurope 2005. (reperibile al seguente indirizzo:http://www.governo.it/GovernoInforma/Dossier/piano_e_europe/eeurope2005_it.pdf). Ciò significa, per esempio, un numero maggiore di aziende attive nel commercio elettronico; scuole non solo collegate ma anche in grado di fare un uso completo di Internet in classe; servizi della pubblica amministrazione disponibili on-line e pienamente interattivi; un maggiore uso di Internet nel settore sanitario, ove esiste una forte domanda di informazioni aggiornate. Occorre più formazione ed occorre intervenire affinché tutti gli europei possano trarre vantaggio dalle possibilità offerte dalle tecnologie digitali.

E-government: progetti di regioni ed enti locali ammessi al finanziamento.

NUMERO SCHEDA: 1992

CLASSIFICAZIONE: E-GOVERNMENT

FONTE: ITALIA OGGI

DATA: 31/10/2002

PAGINA: 33

NATURA ATTO: COMUNICAZIONE

In data 30 ottobre 2002 sono stati presentati dal Ministro per l'Innovazione e le tecnologie i 138 progetti di e-Governament finanziati per complessivi 360 milioni di euro, di cui 120 milioni stanziati dal Ministero ed il resto provenienti da risorse finanziarie da Regioni ed Enti locali. Si tratta del il maggior intervento mai effettuato in Italia in materia di innovazioni e tecnologie nella Pubblica Amministrazione. Il modello di e-Government e' stato messo a punto con l'obiettivo di migliorare il rapporto tra cittadini ed istituzioni, nell'ottica della realizzazione della trasformazione della P.A. verso la nuova concezione di "governo elettronico", che identifica l'innovazione tecnologica come strumento strategico di trasformazione dello Stato e l'avvio della riforma federale, in cui l'architettura istituzionale non e' piu' gerarchica, ma di cooperazione paritaria fra le amministrazioni. I 138 progetti, di cui 98 legati alla realizzazione di servizi a cittadini de imprese e 40 per la creazione di infrastrutture regionali o territoriali, verranno avviati entro la fine del 2002. Gli enti partecipanti ai progetti già finanziati sono 19 regioni, 95 province, 3.574 comuni e 218 comunità montane. Le Regioni e gli Enti locali sono, infatti, attori fondamentali per la realizzazione del piano di e-Government, quali soggetti del decentramento amministrativo.
Il Ministero per l'innovazione e le tecnologie ha pubblicato sul proprio sito istituzionale:
(http://www.mininnovazione.it/ita/egovernment/entilocali/progetti_ammessi.shtml)
una ricerca, aggiornata al 25 febbraio 2005, sullo stato di avanzamento dei progetti su citati.

Si riporta integralmente il documento.

I progetti di e-government ammessi al finanziamento

Il 25 ottobre 2002 la Commissione di Valutazione dei progetti di e-government ha reso pubblica la graduatoria dei progetti presentati dalle Regioni e dagli Enti locali in risposta al primo Avviso per l'erogazione di 120 milioni di euro. Gli enti partecipanti ai progetti finanziati, beneficiari del finanziamento, sono 19 Regioni, 2 Province Autonome, 93 Province, 3574 Comuni e Unioni di Comuni, 218 comunità Montane.
Inoltre, tra i partecipanti ai progetti finanziati vi sono anche: 79 ASL, 22 Università e Istituti scolastici, 16 Amministrazioni Centrali e 8 Prefetture. Sono stati ammessi al cofinanziamento 138 progetti, 40 nella categoria "servizi infrastrutturali" e 98 nella categoria "servizi per cittadini e imprese". Con decreto del 14 novembre 2002, pubblicato nella GU n. 51 del 3 marzo 2003, il Ministro per l'Innovazione e le Tecnologie ha suddiviso il finanziamento complessivo di € 120 milioni in questo modo: € 80 milioni per i 98 progetti che realizzano servizi ai cittadini e alle imprese € 40 milioni per i 40 progetti che realizzano infrastrutture regionali o territoriali. Lo stato di avanzamento dei progetti cofinanziati viene oggi monitorato dall'Ufficio Monitoraggio e gestione progetti delle Regioni e degli Enti Locali del CNIPA.
Ad oggi risultano conclusi 11 progetti (ENTERPRISE, SSB, Sviluppo SIARL, SUAPED, SSB, @LI, MI.PORTI, Comunica, IRIDE, SISTERLAZIO, Portale RL) .
Sono complessivamente 516 (il 12% dei 4195 previsti) i servizi on line realizzati per cittadini/imprese e, per quanto concerne i servizi infrastrutturali, dati molto interessanti riguardano: la distribuzione di 2.7 milioni di carte nazionali dei servizi (CNS) per l'accesso ai servizi on line; la messa in rete di di 11.000 sedi di circa 5.800 diverse amministrazioni per complessivi 175.000 dipendenti pubblici connessi in rete.
Gli ambiti di intervento prioritario (cluster) dei 98 progetti di servizi ai cittadini e alle imprese cofinanziati dall'Avviso sono riportati nella tabella seguente, che indica il numero dei progetti finanziati e il finanziamento complessivo accordato a ciascun cluster.

Servizi per i cittadini/imprese	N. Progetti finanziati	Importo co-finanziato

Informazione e partecipazione	1	€ 110.000,00
Sport, Ambiente, Tempo libero e Beni Culturali	3	€ 580.000,00
Servizi alle imprese	27	€ 13.380.000,00
Servizi per il lavoro	6	€ 5.910.000,00
Portali	44	€ 52.210.000,00
Servizi per la sanità	4	€ 1.870.000,00
Servizi per la scuola	3	€ 1.180.000,00
Giustizia e sicurezza	3	€ 1.160.000,00
Servizi per il sociale	1	€ 340.000,00
Trasferimenti finanziari	3	€ 2.260.000,00
Mobilità e trasporti	3	€ 1.000.000,00

I cluster dei 40 progetti di infrastrutture regionali e territoriali sono riportati nella tabella successiva, che indica il numero dei progetti finanziati e il finanziamento complessivo accordato a ciascun cluster.

Servizi infrastrutturali	N. Progetti finanziati	Importo co-finanziato
Servizi avanzati (sicurezza, certificazione, ...)	6	€ 8.900.000,00
Centri Tecnici	2	€ 1.320.000,00
Interscambio / cooperazione tra amministrazioni	25	€ 21.940.000,00
Servizi di Trasporto	7	€ 7.840.000,00

Il cofinanziamento medio è di 922.000 €, pari al 33% dei costi stimati di progetto. Alle regioni del Centro Nord è andato il 72,44 % dei cofinanziamnti, al Mezzogiorno il 27,56%. Nella tabella seguente è riportata la ripartizione territoriale dei cofinanziamenti del MIT agli Enti partecipanti ai progetti selezionati.

Regione	Finanziamento agli Enti partecipanti
Abruzzo	€ 3.942.006,38
Basilicata	€ 1.056.910,17
Calabria	€ 3.777.429,32
Campania	€ 6.191.977,04
Emilia Romagna	€ 8.605.938,85
Friuli Venezia Giulia	€ 2.007.229,55
Lazio	€ 12.097.036,26
Liguria	€ 4.813.996,53
Lombardia	€ 20.341.338,30
Marche	€ 3.985.250,08
Molise	€ 1.731.893,21
Piemonte	€ 7.571.948,75
Puglia	€ 7.789.088,39
Sardegna	€ 4.115.588,08

Sicilia	€ 9.293.744,25
Toscana	€ 9.267.348,32
Prov. Aut. BZ + Prov. Aut. TN	€ 1.156.932,24
Umbria	€ 2.188.217,15
Valle D'Aosta	€ 271.747,77
Veneto	€ 8.519.727,26

I progetti in corso sono attualmente 134 dal momento che su 138 valutati positivamente dalla Commissione 4 non hanno fatto pervenire la documentazione necessaria per accedere alle tranches di finanziamento. La suddivisione per regione delle graduatorie dei progetti è disponibile nella parte ad accesso riservato del sito dei Centri Regionali di Competenza www.crcitalia.it.

E' stato elaborato un documento sulla formazione di figure professionali per l'attuazione dei progetti di e-government.

NUMERO SCHEDA: 1863

CLASSIFICAZIONE: E-GOVERNMENT

FONTE: IL SOLE 24 ORE

DATA: 27/09/2002

NATURA ATTO: COMMENTO

Al fine di fornire una prima risposta alla conoscenza dei temi attinenti alle nuove competenze nella Pubblica Amministrazione, alla natura dei processi di trasformazione in atto, e ancor più al loro impatto sulla progressiva riorganizzazione e razionalizzazione del personale pubblico dipendente, il tema, il Dipartimento della Funzione Pubblica aveva promosso una ricerca sperimentale "P.A. DUEMILA - I nuovi profili professionali per le Pubbliche Amministrazioni", basata su un sistema di indagine, finalizzata quantificare e qualificare la richiesta di nuove figure professionali nella P.A. La ricerca, affidata all'Istituto G. Tagliacarne - Fondazione dell'Unione Italiana delle Camere di Commercio aveva l'obiettivo di verificare i fabbisogni di professionalità tradizionali ed innovative per il biennio 2001-2002 per le Amministrazioni centrali, le Autonomie locali (Regioni, Province e Comuni secondo un campione definito) e, per una prima verifica sugli Enti pubblici non economici, INPS e INAIL. Dall'indagine è emerso che informatica e tlc sono al secondo posto tra le aree di competenza giudicate necessarie nelle Regioni e al terzo per i Ministeri e le Province. In particolare, le nuove nozioni da padroneggiare all'interno delle pubbliche amministrazioni sarebbero quelle legate a internet e all'infrastruttura tecnologica: reti, banche dati, sviluppo di applicazioni normative per gli enti. Partendo da tali considerazioni, la Microsoft h elaborato un nuovo documento sulla formazione di profili specifici in ambito Ict, in attuazione dei progetti di e-government lanciati dal Governo. Tra le figure che compongono questo modello di competenze vi è quella dell'esperto di tecnologie per i servizi base di e-government, figura di elevata competenza tecnica, responsabile della valutazione e utilizzazione di tecnologie più idonee ad assicurare l'integrità e la provenienza dei documenti informatici (ruolo di

importanza fondamentale, vista la rapida e affermata diffusione della firma digitale).Nell'ambito dell'iniziativa eGovernment.NET per l'Italia, Microsoft ha inoltre realizzato - in collaborazione con HP - un Competence Center che supporterà gratuitamente le PAL nel processo di innovazione tecnologica delle Amministrazioni. All'interno della struttura, consulenti ed esperti tecnologici forniranno ai responsabili degli enti pubblici locali e agli operatori IT le competenze e gli skill necessari per realizzare in piena autonomia progetti di eGovernment facilmente replicabili. Per ulteriori approfondimenti si rimanda al seguente indirizzo Internet: http://www.microsoft.com/italy/pa/

Pubblicate in G.U. le Linee guida in materia di digitalizzazione dell'amministrazione.

NUMERO SCHEDA: 5947

CLASSIFICAZIONE: E-GOVERNMENT

FONTE: ITALIA OGGI

NATURA ATTO: DIRETTIVA

DATA ATTO: 04/01/2005

ORGANO: MINISTERI

Sono state pubblicate sulla Gazzetta ufficiale n. 35 del 12 febbraio 2005 le "Linee guida in materia di digitalizzazione dell'amministrazione" ,contenute nella direttiva del 4 gennaio 2005 emanata dal Ministro per l'innovazione e le tecnologie. Tale direttiva si prefigge di fornire le necessarie indicazioni per la concreta realizzazione dell'obiettivo della digitalizzazione della p.a., al fine di favorire un impiego più efficiente e razionale delle risorse umane e finanziarie e allo scopo di eliminare le disomogeneità attualmente riscontrabili in questo ambito fra le diverse amministrazioni. In particolare, le Linee guida, nell'evidenziare gli apprezzabili risultati già conseguiti, individuano le criticità da risolvere e i traguardi ancora da raggiungere. Fra questi ultimi si segnalano: - la disponibilità on-line di un numero sempre maggiore di servizi prioritari; - l'estensione dell'utilizzo della firma digitale; - l'ampliamento dell'impiego della posta elettronica; - l'ulteriore diffusione delle competenze informatiche acquisite dal personale; - lo sviluppo dell'accesso on-line all'iter delle pratiche, mediante diffusione del protocollo informatizzato, prerequisito della trasparenza amministrativa, e dei call center, utilizzabili anche per verificare lo stato delle pratiche e per la risoluzione dei problemi connessi; - la dotazione dei necessari strumenti di rilevazione della soddisfazione degli utenti, non ancora presenti in tutti gli uffici. Proprio allo scopo di rimediare alle carenze rilevate, ogni Amministrazione dovrà verificare al proprio interno lo stato di attuazione degli obiettivi di legislatura e le ragioni dell'eventuale ritardo, predisponendo un piano di recupero che ne consenta il perseguimento nei tempi stabiliti. Le Linee guida considerano conclusa la prima fase della digitalizzazione della p.a., contraddistinta dalla definizione di un nuovo quadro normativo e dallo sviluppo delle infrastrutture di base, dalla diffusione di conoscenze informatiche tra i

dipendenti, dall'attivazione sia di siti web quali canali di informazione e talora di erogazione di servizi on line agli utenti sia di singoli strumenti e specifici istituti, quali la firma digitale, il protocollo informatico, la posta elettronica certificata, la Carta di identità elettronica e la Carta Nazionale dei Servizi. La seconda fase, il cui presupposto normativo risiede nelle due riforme organiche che costituiscono la base per il futuro sviluppo dell'e-Government (il Sistema Pubblico di Connettività e Cooperazione, destinata a sostituire la Rete Unitaria delle Pubbliche Amministrazioni, e il Codice dell'Amministrazione digitale), produrrà la "dematerializzazione dei documenti" nonché forme di "interazione a distanza, di circolarità e standardizzazione dei dati, di multicanalità, di accessibilità, di nuove competenze professionali". In pratica, la digitalizzazione della p.a. consentirà ai cittadini di interagire con qualunque amministrazione attraverso la rete a fronte di un imponente sforzo organizzativo di tutte le p.a. per rendere sempre disponibili tutte le informazioni in modalità digitale. Le Linee guida passano poi a illustrare le aree di intervento per l'effettiva realizzazione del progetto di digitalizzazione della p.a.. Ad essere interessati sono i settori della comunicazione elettronica, della Rete Internazionale delle pubbliche amministrazioni, del sistema pubblico di connettività e cooperazione, della Carta Nazionale dei Servizi, dei servizi on line agli utenti e della gestione documentale.
Con riguardo all'aspetto finanziario, le Linee guida rinviano a successivi DPCM la predisposizione di un programma strutturale per l'informatica pubblica volta a razionalizzarne i costi senza comprimerne l'impulso all'innovazione e allo sviluppo di soluzioni tecnologiche e organizzative innovative. Per evitare che tale sviluppo produca un incremento della spesa informatica e nell'intento di conseguire economie gestionali, le Linee guida suggeriscono l'adozione di precise modalità di approvvigionamento dei servizi, un'attiva collaborazione con il CNIPA e l'impiego della tecnologia "Voice over IP", che consente il trasferimento delle conversazioni vocali mediante server di rete in luogo di centrali telefoniche e centralini. L'adozione di questa tecnologia consente di ricorrere ad un collegamento unico per qualsiasi tipo di comunicazione (voce, dati e immagini) attraverso il Sistema Pubblico di Connettività e la Rete Internazionale delle Pubbliche Amministrazioni, con indubbi vantaggi, a parità di qualità del servizio, per i costi di telefonia, gestione e manutenzione.
Infine, le Linee guida attribuiscono un ruolo determinante per la riuscita della digitalizzazione della p.a. al coinvolgimento dei dirigenti, ai quali dovranno essere assegnati idonei obiettivi da realizzare nel corso del 2005.

Si riporta il testo della sentenza in esame. Si segnala un commento alla direttiva sulla rivista "Guida agli Enti Locali", n. 14 del 9 aprile 2005, pp. 58-60, a cura di P. Subioli, consultabile presso il settore Studi e documentazione legislativi.
Si riporta altresì il testo della direttiva:

Direttiva del 4 gennaio 2005

LINEE GUIDA IN MATERIA DI DIGITALIZZAZIONE DELL'AMMINISTRAZIONE (Gazzetta Ufficiale n. 35 del 12 febbraio 2005)
IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE

premessa

La presente direttiva è indirizzata a tutte le Amministrazioni dello Stato e a tutti gli Enti pubblici

sottoposti a vigilanza ministeriale. Per le Regioni e gli Enti locali costituisce contributo alle determinazioni in materia, nel rispetto della loro autonomia amministrativa, e sarà oggetto di successivo atto di indirizzo ai sensi dell'articolo 29, comma 7, della legge 23 dicembre 2001, n. 448 (legge finanziaria per il 2002). Può rappresentare schema di riferimento anche per le altre amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165. Le precedenti direttive 1 e gli altri atti di indirizzo in materia di digitalizzazione, emanati anche in relazione a specifici settori, devono, comunque, intendersi validi ed efficaci e costituiscono parte integrante delle seguenti disposizioni.

1. STATO DI ATTUAZIONE DEGLI OBIETTIVI DI DIGITALIZZAZIONE. La rilevazione sullo stato di attuazione degli obiettivi di legislatura nella pubblica amministrazione ha evidenziato il raggiungimento di significativi risultati. Permangono, peraltro, disomogeneità tra le diverse amministrazioni. In particolare si segnalano di seguito i principali risultati conseguiti e le maggiori criticità da affrontare: a) circa il 50% dei servizi prioritari sono disponibili on-line, altri sono disponibili solo parzialmente. Per quelli rispetto ai quali si registrano criticità le Amministrazioni dovranno effettuare un'analisi puntuale dei motivi di ritardo, e produrre un piano al fine di accelerarne la realizzazione. E' in ogni caso opportuno attivare la verifica della soddisfazione dell'utente; 1Direttiva del 21 dicembre 2001, pubblicata in Gazzetta Ufficiale del 5 febbraio 2002 n. 30; Direttiva del 20 dicembre 2002, pubblicata in Gazzetta Ufficiale del 4 marzo 2003 n. 52 Direttiva del 18 dicembre 2003, pubblicata in Gazzetta Ufficiale del 4 febbraio 2004 n. 28

2. OBIETTIVI DI DIGITALIZZAZIONE PER LA LEGISLATURA indicati nelle "Linee guida del Governo per lo sviluppo della Società dell'Informazione" pubblicate sul sito www.innovazione.gov.it: Servizi online ai cittadini e alle imprese 1. Tutti i servizi "prioritari" disponibili on-line 2. 30 milioni di Carte di Identità Elettroniche e Carte Nazionali dei Servizi distribuite 3. 1 milione di firme digitali diffuse entro il 2003 Efficienza interna della Pubblica Amministrazione 4. 50% della spesa per beni e servizi tramite eProcurement 5. Tutta la posta interna alla Pubblica Amministrazione via e-mail 6. Tutti gli impegni e mandati di pagamento gestiti on-line Valorizzazione delle Risorse Umane 7. Alfabetizzazione certificata di tutti i dipendenti pubblici eleggibili 8. 1/3 della formazione erogata via eLearning Trasparenza 9. 2/3 degli uffici della Pubblica Amministrazione con accesso on-line all'iter delle pratiche da parte dei cittadini Qualità 10. Tutti gli uffici che erogano servizi dotati di un sistema di soddisfazione dell'utente. b) sono state distribuite oltre 1,6 milioni di carte di firma digitale. Il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) ha distribuito oltre 23.000 smart card ad altrettanti funzionari pubblici, con le quali vengono firmati digitalmente ogni giorno circa 3.000 mandati di pagamento. E' necessario rivedere le procedure amministrative al fine di estendere rapidamente l'utilizzo della firma digitale; c) l'utilizzo della posta elettronica è sensibilmente aumentato nelle comunicazioni interne alla Pubblica Amministrazione. Poiché il completamento dell'Indice PA (elenco di tutti gli uffici pubblici con casella di posta elettronica a disposizione del pubblico), attualmente in corso di predisposizione ad opera del CNIPA, costituirà certamente un incentivo all'uso di tale strumento, si invitano le Amministrazioni che non abbiano ancora ottemperato all'invio dei dati ad attivarsi in tal senso con la massima urgenza garantendo, altresì, il tempestivo e costante aggiornamento dei dati stessi; d) sempre nel settore della posta elettronica, va segnalato che molte amministrazioni hanno avviato iniziative per accrescere l'efficienza e ridurre i costi di proprie attività sostituendo ad operazioni materiali il ricorso a comunicazioni elettroniche. In questo ambito si colloca anche l'iniziativa denominata @P@3, finalizzata a cofinanziare specifici progetti delle Amministrazioni. E' allo studio la possibilità di rilanciare il progetto per ulteriori iniziative di razionalizzazione e risparmi; e) attualmente 25 milioni di impegni e mandati di pagamento sono on line. Nel corso del 2004 si è, infatti, esteso l'uso del Sicoge a quasi tutte le amministrazioni centrali (coprendo quasi il 100% dei capitoli di spesa delle stesse). Inoltre è stata automatizzata anche la gestione degli ordini di accreditamento che, a partire da giugno, comporta la gestione telematica di circa 175 mila ordini di accreditamento annuali; occorre però ancora estendere tali sistemi alle contabilità speciali; f) le competenze informatiche acquisite dal personale pubblico sono molto diffuse; i dati sulla formazione a distanza (e-learning) indicano una crescita superiore al 60% sebbene permanga poco rilevante il numero delle certificazioni tipo ECDL o equivalenti; g) l'accesso on-line all'iter delle pratiche mostra difficoltà legate al notevole impatto organizzativo. E' comunque in crescita la diffusione del protocollo informatizzato, prerequisito della trasparenza amministrativa. Nei settori nei quali è maggiore l'esigenza dei cittadini, ad es. fisco e previdenza, sono pienamente operativi call center utilizzabili anche per verificare lo stato delle pratiche e risolvere i problemi connessi. Per le Amministrazioni che non abbiano ancora completato l'automazione della gestione documentale e del protocollo informatico si segnala che il CNIPA propone tale servizio in modalità ASP 4; h) non sono

ancora presenti in tutti gli uffici i necessari strumenti di rilevazione della soddisfazione degli utenti. 3 Progetto approvato dal Comitato dei Ministri per la Società dell'Informazione il 18 marzo 2003 pubblicato sul sito www.cnipa.gov.it. 4 ASP (Application Service Provider): servizi resi disponibili in rete per le amministrazioni, le quali possono acquisirli senza dover sviluppare soluzioni proprie e senza acquistare hardware e licenze software. Azioni conseguenti – Piani di recupero Ogni Amministrazione dovrà verificare al proprio interno lo stato di attuazione degli obiettivi di legislatura, i motivi del mancato o parziale raggiungimento, e predisporre un Piano di recupero che ne consenta il conseguimento nei tempi stabiliti. Detti Piani di recupero costituiranno parte integrante del Piano esecutivo per le tecnologie dell'informazione e della comunicazione (ICT) per il 2005 da trasmettere al CNIPA entro il 31 gennaio del 2005, redatto secondo le modalità stabilite al punto 6 della direttiva del 18 dicembre 2003. 3. LA SECONDA FASE DELLA DIGITALIZZAZIONE DELLA P.A. Gli anni 2001-2004 hanno rappresentato la prima fase della digitalizzazione della Pubblica Amministrazione, nella quale l'impegno del Governo e delle amministrazioni è stato rivolto, soprattutto, al riorientamento ai servizi, allo sviluppo delle infrastrutture di base, alla diffusione di competenze informatiche e di una crescente familiarità con gli strumenti informatici tra i dipendenti e, nel periodo più recente, all' attivazione di siti web come canali di informazione ed in alcuni casi di erogazione di servizi on line agli utenti. In questa fase si è, quindi, pervenuti ad una maggiore diffusione, negli uffici e nei processi di lavoro, dell'uso delle ICT. Le basi di questo importante processo di crescita sono state consapevolmente tracciate non solo e non tanto in disposizioni legislative, quanto – piuttosto – innescando un circuito virtuoso "definizione di obiettivi – attuazione – controllo" nelle amministrazioni, sostenuto anche attraverso il cofinanziamento di iniziative di innovazione proposte dalle stesse amministrazioni, sia centrali (attraverso deliberazioni del Comitato dei Ministri per la Società dell'Informazione) che locali (programma di e-Government). Nel frattempo, come noto, sono stati disciplinati singoli strumenti e specifici istituti che connotano la digitalizzazione dell'Amministrazione (firma digitale, protocollo informatico, posta elettronica certificata, Carta di identità elettronica e Carta Nazionale dei Servizi, ecc.). Questa prima importante fase della digitalizzazione della Pubblica Amministrazione può essere considerata conclusa. Infatti, sulla base del patrimonio di esperienze maturate, ha preso corpo la definizione di una nuova cornice normativa, che induce le amministrazioni a non adottare gli strumenti offerti dalle tecnologie dell'informazione e della comunicazione quali "possibilità aggiuntive" dell'azione amministrativa, ma a sostituire gli strumenti e le modalità tradizionali di rapporto con gli utenti e di svolgimento delle attività interne. E' ora il momento di attivare la seconda fase, che dovrà essere improntata alla piena valorizzazione degli investimenti già realizzati, alla razionalizzazione del sistema nel suo complesso, alla interoperabilità tra le amministrazioni, alla effettiva ed ampia transizione verso modalità di erogazione dei servizi on line e, infine, al raccordo pieno tra digitalizzazione, organizzazione, processi e servizi al pubblico. Questo passaggio dalla prima alla seconda fase della digitalizzazione trova la sua cornice normativa nell'approvazione di due riforme organiche che costituiranno la base per l'evoluzione dell'e-Government nei prossimi anni. La prima riforma è contenuta nel decreto legislativo sul Sistema Pubblico di Connettività e Cooperazione, ormai vicino alla definitiva adozione e che sostituirà, nello spirito di una visione pienamente condivisa tra Stato, Regioni ed Enti Locali, la Rete Unitaria delle Pubbliche Amministrazioni. Il nuovo sistema raccorderà tutte le pubbliche amministrazioni statali, regionali e locali. La seconda riforma è costituita dal "Codice dell'Amministrazione digitale"5, che darà un assetto unitario ed organico al complesso di diritti dei cittadini e delle imprese, agli istituti giuridici ed ai doveri delle amministrazioni in materia di digitalizzazione delle pubbliche amministrazioni. La prossima approvazione del decreto legislativo costituisce l'inizio di una seconda fase della digitalizzazione delle pubbliche amministrazioni, in quanto rende obbligatoria l'innovazione nella Pubblica Amministrazione nel modo più naturale: da una parte dando ai cittadini il diritto di interagire sempre, ovunque e verso qualunque amministrazione attraverso la rete; dall'altra, stabilendo che tutte le amministrazioni devono organizzarsi in modo da rendere sempre e comunque disponibili tutte le informazioni in modalità digitale. Nuovi principi I decreti legislativi concernenti il Sistema Pubblico di Connettività e Cooperazione (SPC) e il Codice dell'Amministrazione digitale forniranno l'adeguato supporto normativo in materia di dematerializzazione dei documenti, di comunicazione elettronica, di interazione a distanza, di circolarità e standardizzazione dei dati, di multicanalità, di accessibilità, di nuove competenze professionali. In relazione a tali nuovi principi, le Amministrazioni pubbliche, anche con il supporto del CNIPA, dovranno, nel corso dell'anno 2005, porre in essere tutte le azioni di competenza per cogliere appieno le opportunità offerte dai nuovi strumenti. In tale contesto, sarà necessario perseguire una piena integrazione degli interventi di digitalizzazione con le politiche di riforma delle pubbliche amministrazioni, con specifico riferimento alla semplificazione delle procedure e dell'organizzazione

amministrativa ed alla formazione del personale. In particolare, le amministrazioni, nel programmare i loro interventi di digitalizzazione, dovranno segnalare al Dipartimento della funzione pubblica ed al Ministro per l'innovazione e le tecnologie sia le opportunità/necessità di semplificazione dei procedimenti amministrativi e delle regolamentazioni interne, sia i fabbisogni di nuove competenze, ai fini della adozione degli interventi conseguenti. 5 Lo schema di decreto legislativo, recante il Codice dell'Amministrazione digitale, è stato approvato in via preliminare dal Consiglio dei Ministri in data 11 novembre 2004 Settori di intervento Le seguenti aree costituiscono settori di intervento essenziali alla realizzazione della seconda fase della digitalizzazione. Essi richiedono uno sforzo sinergico da parte delle singole Amministrazioni al fine di dare esecuzione alle azioni previste dalla normativa vigente e per la realizzazione delle quali il CNIPA ha impegnato le proprie risorse ed avviato le necessarie attività progettuali: Comunicazione elettronica Nel rammentare la direttiva concernente l'impiego della posta elettronica nelle pubbliche amministrazioni6, nonché le norme relative all'utilizzo della firma digitale, si fa presente che sono di prossima definitiva approvazione le disposizioni necessarie per assicurare piena validità giuridica alle comunicazioni per via elettronica7, sia all'interno di ciascuna amministrazione, sia tra amministrazioni diverse, sia, infine, tra amministrazioni, cittadini e imprese. Di conseguenza diviene necessario riorganizzare il lavoro all'interno delle amministrazioni per sviluppare l'uso degli strumenti telematici, sostenendo minori oneri per la spedizione e l'archiviazione con notevoli vantaggi di velocità dell'azione amministrativa. Rete Internazionale delle pubbliche amministrazioni Per avvalersi dei previsti finanziamenti del CNIPA, le Amministrazioni che necessitano di connettività internazionale dovranno sottoscrivere i contratti di fornitura con l'aggiudicatario entro il primo trimestre del 2005. Sistema Pubblico di Connettività e Cooperazione Nelle more dell' attuazione del nuovo sistema, le Amministrazioni dovranno pianificare la migrazione dalla Rete Unitaria verso il nuovo Sistema Pubblico di Connettività e Cooperazione (SPC) presentando al CNIPA i relativi piani entro il 2005, al fine di non superare il termine di sei mesi dalla data del contratto quadro che sarà stipulato dal CNIPA. 6 Direttiva del 27 novembre 2003 pubblicata in Gazzetta Ufficiale del 12 gennaio 2004 n. 8 7 Schema di DPR sull'utilizzo della Posta Elettronica Certificata (PEC) approvato in via preliminare dal Consiglio dei Ministri del 25 marzo 2004 Carta Nazionale dei Servizi (CNS) Sono ormai definite con decreto dei Ministri dell'Interno, per l'innovazione e tecnologie, dell'economia e delle finanze, datato 9 dicembre 2004, 8 le regole tecniche sulla CNS; le amministrazioni dovranno, pertanto, programmare l'emissione della CNS in sostituzione di altri strumenti di accesso ai servizi sino ad ora realizzati, tenendo comunque presente che, ai sensi della normativa vigente, ogni Amministrazione deve, comunque, garantire l'accesso ai propri servizi da parte dei titolari di CNS. Al fine di promuoverne la diffusione il CNIPA definirà un contratto quadro per la fornitura di CNS al quale le pubbliche amministrazioni potranno aderire. Servizi on line agli utenti Si conferma la priorità di favorire la diffusione e l'utilizzo di servizi on line per cittadini ed imprese, per migliorare il servizio e ridurre i costi. Le amministrazioni dovranno, pertanto, curare la realizzazione e la promozione di servizi interattivi, assicurando, nel contempo, la possibilità di accesso attraverso una pluralità di canali (internet, telefonia mobile, telefonia fissa, tv digitale), ciascuno facoltativamente fruibile dagli utenti. In tale ottica le amministrazioni dovranno collaborare per integrare i procedimenti di rispettiva competenza, al fine di agevolare gli adempimenti richiesti alle imprese e accrescere l'efficienza nelle aree che coinvolgono più amministrazioni, attraverso la definizione e l'attuazione di accordi per la partecipazione al sistema di cooperazione attuato nell'ambito del Sistema per i servizi integrati alle imprese (www.impresa.gov.it). Gestione documentale Le amministrazioni dovranno porre in atto tutte le misure previste dalla normativa in materia di gestione documentale eventualmente avvalendosi dei servizi resi disponibili dal CNIPA nell'ambito dell'iniziativa Servizio di gestione del Protocollo Informatico e gestione documentale in modalità ASP. 3. RISPARMI e RAZIONALIZZAZIONE L'articolo 1, commi da 192 a 196, della legge finanziaria per il 2005, introduce nuovi modelli di comportamento per le pubbliche amministrazioni finalizzati alla razionalizzazione dei processi operativi e, conseguentemente, al contenimento della spesa. La sua attuazione avverrà attraverso l'emanazione di successivi DPCM che individueranno le aree prioritarie e l'ambito soggettivo di intervento, al fine di predisporre un programma strutturale per l'informatica pubblica e la sua contestuale razionalizzazione, mantenendo l'attuale impulso all'innovazione, accelerando lo sviluppo e la diffusione di soluzioni tecnologiche e organizzative innovative, evitando, altresì, che questo sviluppo si traduca in incremento della spesa informatica e, al contrario, producendo economie. Ciò sarà possibile utilizzando le nuove modalità di approvvigionamento dei servizi che semplificano le incombenze delle singole amministrazioni, anche assumendo come modello di riferimento quello dei servizi ASP. Per la migliore attuazione della nuova disciplina introdotta dalla legge finanziaria è auspicabile un'attiva collaborazione con il CNIPA da parte delle Amministrazioni che potranno contribuire a determinarne

gli ambiti di azione, effettuando una accurata analisi della propria situazione in rapporto all'utilizzo delle ICT al fine di individuare: -i casi di duplicazione o ridondanza di sistemi e strutture informatiche, sui quali sia possibile intervenire per razionalizzare e conseguire economie gestionali; -i casi in cui sia possibile ed opportuno utilizzare soluzioni condivise o soluzioni già adottate in altre amministrazioni. E' da sottolineare la possibilità di conseguire economie anche attraverso l'applicazione della Direttiva inerente l'acquisizione del software9, da effettuarsi attraverso una valutazione comparativa che tenga anche conto di prodotti disponibili in riuso od a codice sorgente aperto. E' all'uopo disponibile una proposta di metodologia di valutazione messa a punto dal CNIPA. Nell'ambito delle iniziative tendenti alla razionalizzazione ed al risparmio, particolare importanza assume l'adozione della tecnologia "Voice over IP", che consente di trasportare le conversazioni vocali via Internet o su reti per trasmissione dati che operano in modo analogo ad Internet, impiegando router e server di rete in luogo di centrali telefoniche e centralini. I centralini, pertanto, vengono sostituiti da server, utilizzando, di norma, il cablaggio esistente ed eliminando così costose duplicazioni. L'adozione di questa tecnologia consente di ricorrere ad un collegamento unico per qualsiasi tipo di comunicazione (voce, dati e immagini), attraverso il Sistema Pubblico di Connettività e la Rete Internazionale delle Pubbliche Amministrazioni, che sono state progettate per un trasporto di qualità per ciascuna delle indicate tipologie di comunicazioni. I vantaggi concreti potenzialmente derivanti dall'adozione del Voip consistono in una notevole riduzione delle spese di telefonia, oltre che delle spese di gestione e manutenzione, a parità di qualità del servizio, grazie : -all'azzeramento dei costi delle conversazioni all'interno delle amministrazioni nonché alla riduzione dei costi delle chiamate verso l'esterno; -alla riduzione dei costi di gestione per l'impiego di un unico cablaggio e di impianti della stessa tipologia per voce e dati; -all'azzeramento dei costi legati agli spostamenti delle connessioni telefoniche del personale che possono essere realizzati con un semplice comando via software. Le Pubbliche Amministrazioni con contratti in scadenza a breve in questo settore dovranno valutare, prima del rinnovo dei contratti stessi, la convenienza del passaggio alle nuove tecnologie, anche avvalendosi dell'apposito Centro di Competenza, all'uopo istituito presso il CNIPA che potrà fornire, anche, supporto alla pianificazione dell'introduzione della tecnologia Voip ed alla sostituzione degli impianti esistenti, da programmare nell'arco di tre anni. 8 Decreto pubblicato sui siti: www.innovazione.gov.it e www.cnipa.gov.it. 9 Direttiva del 19 dicembre 2003 "Sviluppo ed utilizzazione dei programmi informatici da parte delle pubbliche amministrazioni" pubblicata in Gazzetta Ufficiale del 7 febbraio 2004 n. 31

4. RUOLO DELLA DIRIGENZA . Per la realizzazione dei citati obiettivi e per il successo della seconda fase di digitalizzazione dell'Amministrazione, appare necessario il più ampio coinvolgimento dei dirigenti ai quali dovranno essere, conseguentemente, assegnati corrispondenti obiettivi da realizzare nel corso dell'anno. Tale coinvolgimento dovrà mirare ad ottenere, da parte della dirigenza, non soltanto il raggiungimento degli obiettivi prefissati, ma anche a suscitare un atteggiamento propositivo per la definizione dei programmi strategici delle singole Amministrazioni. Ogni dirigente di vertice delle strutture in cui si articola ciascuna amministrazione dovrà essere responsabilizzato per la definizione e per il raggiungimento di precisi obiettivi nei settori indicati dalla presente direttiva, indicando i conseguenti risparmi e le esigenze di formazione del personale. Appare, infatti, indispensabile curare che, attraverso un adeguato programma di formazione tecnica, giuridica e organizzativa, sia assicurato un livello di conoscenza tale da porre la dirigenza in condizione di essere essa stessa motore del cambiamento in atto nell'agire dell'Amministrazione.

Roma, 4 gennaio 2005 Lucio Stanca.

Il TAR Lazio, con sentenza n. 2159 del 08/03/2004, ha stabilito che la disponibilità del bando sul sito internet dell'ente pubblico è sufficiente per l'osservanza del principio della pubblicità adeguata.

NUMERO SCHEDA: 4509

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: TAR LAZIO

DATA: 08/03/2004

RIFERIMENTO NORMATIVO: legge 241/90 e d.lgs. 123/98

NATURA ATTO: SENTENZA

DATA ATTO: 08/03/2004

NUM. ATTO: 2159

ORGANO: TAR LAZIO

La sentenza n. 2159 del TAR Lazio ha affermato che la pubblicazione di un bando sulla gazzetta ufficiale con rinvio alla pubblicazione sul sito internet, non comporta alcuna violazione dell'art. 12 legge 241/90 né dell'art. 5 d.lgs. 123/98, secondo cui la pubblica amministrazione deve predeterminare i requisiti, le modalità e i criteri di attuazione attraverso la pubblicazione in Gazzetta Ufficiale. Pertanto l'avviso che compare sulla gazzetta ufficiale che rinvia al documento integrale consultabile sul sito internet. Il TAR respingendo il ricorso di un consorzio di cooperative onlus contro Sviluppo Italia e il ministero del Lavoro ha stabilito che l'home page dell' ente e la gazzetta ufficiale hanno la stessa dignità.

Si allega il testo della sentenza n. 2159 del 08/03/2004 del TAR Lazio.

S E N T E N Z A

DIRITTO

Il Consorzio Fraternità Creativa e le Cooperative indicate in epigrafe, in via principale, impugnano il provvedimento ed i relativi atti presupposti, con cui Sviluppo Italia S.pA. ha deliberato la "non accoglibilità" della richiesta di finanziamento del progetto "Un grappolo bresciano" . In particolare il rigetto dell'istanza è affidato alla duplice considerazione che: -- non sussistevano "i requisiti di cui all'art. 4, relativamente alla non prevedibilità, se non per un consorzio, di essere tutorato da un altro consorzio" avendo il Consorzio di cooperative sociali previsto di svolgere attività di tutoraggio di una cooperativa sociale; -- il progetto difettava anche dei requisiti "di cui all'art. 5 del Bando, relativamente alla operatività integrata delle iniziative". 1. Deve preliminarmente d'ufficio rilevarsi, quanto alla giurisdizione, che con sentenza n. 6412 del 25 luglio 2000 (integralmente confermata dal C.d.S. - Sesta Sez. con decisione n. 192 del 22 gennaio 2001), la Sezione ha già ritenuto la propria giurisdizione -- sia pure nei riguardi della Società formalmente dante causa di Sviluppo Italia S.p.A. -- in relazione alla natura di "organismo di diritto pubblico" in senso tecnico. La Società resistente infatti svolge, sia pure nelle forme di persona giuridica privata, funzioni di sostegno all'economia (selezione e l'incentivazione dell'attività produttiva con contribuzione nazionale e comunitaria) che hanno natura squisitamente pubblicistica a nulla rilevando che la soddisfazione di bisogni generali non esaurisca l'ambito di attività della stessa. Per tale ragione, anche quando la distribuzione di risorse erariali avvenga con la formula del prestito (modalità del resto utilizzata dal Tesoro fin dagli anni trenta del secolo scorso) tali funzioni non possono essere assolutamente equiparate ad un'attività finanziaria e bancaria (che è invece connotata dall'esclusivo rilievo del conseguimento del profitto) per cui anche l'ottenimento dell'autorizzazione ad operare ai sensi del testo unico delle leggi in materia bancaria e creditizia emanato con d.lg. 1 settembre 1993 n. 385, è irrilevante ai fini del radicamento della giurisdizione. 2. Nel merito, il ricorso è infondato. Con il primo motivo di gravame si deducono due differenti profili di ricorso che vanno partitamene confutati. Viene lamentata innanzitutto la violazione dell'art. 2, II° della L. n. 241/1990 che impone la fissazione del termine di conclusione del procedimento. La censura è inconferente sul piano della legittimità per provvedimento di non ammissione al contributo. Come la giurisprudenza ha da tempo chiarito, il mancato rispetto del termine previsto dall'art. 2, comma 3, l. 7

agosto 1990 n. 241 per la conclusione dei procedimenti amministrativi determina solo l'illegittimità del silenzio mantenuto dalla p.a. e non anche l'illegittimità del provvedimento tardivamente assunto. E ciò perché il termine per la definizione del procedimento ha carattere meramente acceleratorio, non recando la predetta legge alcuna prescrizione sulla perentorietà del temine, sulla decadenza della potestà amministrativa, o sull'illegittimità del provvedimento adottato (cfr. T.A.R. Lazio, sez. III, 15 gennaio 2003, n. 128; T.A.R. Veneto, sez. I, 20 gennaio 2003, n. 529; T.A.R. Liguria, sez. II, 5 luglio 2002, n. 801, Consiglio Stato, sez. V, 3 giugno 1996, n. 621). Si sostiene poi l'illegittimità dell'intera procedura, in quanto sulla G.U. parte II° n. 170 del 24 luglio 2001, in luogo del Bando vero e proprio era stato pubblicato un "avviso" il quale rinviava ad un documento "Modalità di presentazione dei progetti" consultabile sul sito internet di Sviluppo Italia. Tale modalità procedimentale, ad avviso dei ricorrenti, avrebbe violato il combinato disposto dell'art. 12 della L. n. 241/1990 in base al quale l'amministrazione deve predeterminare e pubblicare i criteri per l'erogazione dei contributi; e dell'art. 5 del d.lgs. n. 123/1998 che pone il principio generale dell'ordinamento per cui i requisiti, le modalità e le condizioni concernenti gli interventi attuati con procedimento valutativo debbono esser resi noti con pubblicazione sulla Gazzetta ufficiale. Il rinvio al sito internet non poteva quindi esser legittimamente sostitutivo della sua integrale pubblicazione, non potendo il supporto elettronico garantire i profili di diffusione e di pubblica accessibilità tipici della Gazzetta Ufficiale né tantomeno il carattere dell'ufficialità e della immodificabilità che la pubblicazione conferisce, specialmente con riguardo alle predeterminazione dei criteri di valutazione. L'assunto non merita adesione. a) Il principio della "pubblicità adeguata" può dirsi legittimamente assicurato dall'uso del sito internet, dato che il rinvio ad atti, liberamente consultabili sulla rete informatica, di per sé, non costituisce una fattore di diminuzione delle garanzie procedimentali. L'art. 9 del d.P.R. 28 dicembre 2000 n. 445 concernente il Testo Unico in materia di documentazione amministrativa,infatti, dispone: -- al primo comma, che gli atti amministrativi informatici "costituiscono informazione primaria ed originale", sancendo così il principio di piena equiparazione sul piano giuridico tra atti amministrativi cartacei e degli atti amministrativi elettronici (la cui accessibilità sulla rete web consente anzi agli interessati sia di conoscere direttamente, ed in tempo reale, tutti i provvedimenti di loro interesse, che di poter gestire i relativi procedimenti); -- al terzo comma, il principio, di carattere funzionale ed organizzatorio, per cui le pubbliche amministrazioni provvedono a definire, ed a rendere disponibili, per via telematica "moduli e formulari". Non essendo poi stata allegata dal Consorzio ricorrente alcuna concreta impossibilità, nemmeno temporanea, di loading delle informazioni del bando e delle istruzioni applicative, non ha alcun fondamento giuridico la pretesa mancanza di garanzie di accessibilità al sito internet di Sviluppo Italia non sovvenendo ragioni per ritenere che la gestione di detto sito non abbia rispettato le modalità di cui alla Direttiva del 09/12/2002 sulla "Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali" del Ministero per l'Innovazione Tecnologica. Neppure le generiche affermazioni circa la mancanza di garanzie dei documenti pubblicati, possono aver rilievo giuridico, non avendo la parte ricorrente al riguardo indicato alcuna modifica in concreto degli atti pubblicati sul sito. Perde, pertanto consistenza l'obiezione che nell'avviso pubblicato nella Gazzetta Ufficiale fossero assenti i criteri di valutazione dato che tali elementi erano puntualmente contenuti negli atti pubblicati sul sito (cfr. art. 8 del bando di gara, e le pagg. 14 e segg. della Guida esplicativa: all. 3 al deposito Sviluppo Italia del 24 febbraio 2003). L'onere di pubblicità del procedimento di cui all'art. 12 della L. n. 241/1990 é legittimamente assolto con la pubblicazione sulla G.U. di un avviso diretto a rendere nota l'esistenza di un procedimento per la concessione di benefici di carattere finanziario, se tale avviso è accompagnato con la messa in libera consultazione sul sito elettronico del bando integrale, delle istruzioni applicative e dei modelli da compilare. b) Del tutto inconferente è poi, la denunciata violazione dell'art. 5 del Decreto legislativo 31 marzo 1998, n. 123. In assenza di un diretto e specifico richiamo nel bando, deve escludersi la diretta ed immediata applicabilità alla procedura in questione del d.lgs. n. 123/1998, il quale concerne esclusivamente gli ausili finalizzati al sostegno economico delle "imprese" da parte del Ministero delle Attività Produttive. Invece il Bando in questione aveva come finalità il sostegno delle attività di inserimento sociale delle persona svantaggiate, da parte del Ministero del Wellfare e non dell'incentivazione delle attività economiche delle imprese,. Peraltro, si deve rilevare che l'art. 5, erroneamente invocato dalla parte ricorrente, non impone assolutamente l'integrale pubblicazione di tutti gli elementi rilevanti ai fini della selezione nella G.U. ma invece prescrive proprio che "Il soggetto competente comunica i requisiti, le modalità e le condizioni concernenti i procedimenti di cui ai commi 2 e 3, con avviso da pubblicare nella Gazzetta Ufficiale della Repubblica italiana almeno novanta giorni prima dell'invio delle domande, e provvede a quanto disposto dall'art. 2, comma 3". Il riferimento alla pubblicazione di un "avviso" e non di un "bando" non consente di poter condividere l'assunto di parte ricorrente circa la necessità di una pubblicazione integrale del bando. Quando il legislatore utilizza il

termine “bando” vuole che debbano esser resi noti tutti gli elementi fondamentali del procedimento (e questo il caso ad esempio dell’art. 8 secondo comma d.lgs. n. 157/1995); mentre ricorre alla locuzione “avviso” quando ritiene sufficiente che venga data pubblica notizia del procedimento, rinviando ad altri atti per i dettagli (cfr. ad es. art. 5 primo comma d.lgs. n. 358/1995; art. 8 primo e secondo comma del d.lgs. n. 157 cit.). L’obbligo procedimentale di pubblicità del procedimento, è esclusivamente limitato alla pubblicazione di una comunicazione (circa l’esistenza e la scadenza del bando per il finanziamento delle iniziative) che assicuri la conoscibilità del procedimento e quindi la par condicio di tutti i soggetti potenzialmente interessati all’inserimento in graduatoria. In conclusione il motivo è complessivamente infondato e deve essere respinto. 3. Parimenti privo di pregio giuridico appare il secondo motivo con cui il Consorzio ricorrente lamenta che, incongruamente, la S.I. avrebbe ritenuto la pretesa inidoneità di un consorzio a svolgere il tutoraggio di una cooperativa, in quanto: -) l’art. 4 del Bando, imponeva che il “tutoraggio” di ogni nuova realtà avrebbe dovuto “essere affidata ad un soggetto dotato di adeguata esperienza e di adeguati livelli dimensionali e di efficienza” quale proprio il ricorrente Consorzio; -) non vi sarebbe alcuna ragione logica dell’affermazione per cui un consorzio (come quello ricorrente, con un’esperienza imprenditoriale più che triennale) non sarebbe stato in grado di esercitare il trasferimento di capacità, esperienza progettuale, e Know-how organizzativo e gestionale nei riguardi di una sola cooperativa. Irragionevolmente si sarebbe adottato un criterio meramente formale per poter aprioristicamente escludere il progetto “Un Grappolo Bresciano”. L’assunto non ha complessivamente pregio. In primo luogo l’inequivoca espressione della "lex specialis" del procedimento era tale da ingenerare, nei partecipanti, un assoluto convincimento sulla necessità di redigere le offerte secondo la precisa formulazione dell’art. 4 del bando, che imponeva ad un consorzio di tutelare un altro consorzio e non anche delle cooperative. La prescrizione era tale da non consentire margini interpretativi nè per Sviluppo Italia che -- una volta posta la norma -- non avrebbe comunque potuto discostarsene; e neppure per gli interessati i quali avrebbero dovuto: o adeguare il progetto alla regola (per esempio indicando, quali tutor delle cooperative sociali, alcune delle imprese costituenti il consorzio delle cooperative sociali); ovvero previamente impugnare una clausola che influiva direttamente sulla ammissibilità stessa del progetto. Del tutto erroneamente il consorzio -- sulla base di una sua autonoma, soggettiva, valutazione di illogicità della prescrizione -- ha ritenuto di poter del tutto prescindere da una disposizione cogente sulla strutturazione del progetto. Sul piano della ragionevolezza delle scelte, peraltro, la valutazione circa la maggiore efficacia dell’azione di supporto all’avvio di una cooperativa sociale operata da un tutor costituito in forma di cooperativa sociale, afferisce a valutazioni di amplia discrezionalità amministrativa, ma non pare violi manifestamente i precetti della logica e della razionalità. Appare ragionevole che, i consorzi di cooperative sociali facciano da tutor solo ed esclusivamente ad un altro “consorzio di cooperative” (cioè ad un omologa struttura interorganizzativa diretto alla fornitura di servizi consulenziali e di promozione imprenditoriale a favore delle cooperative aderenti); e non possano supportare le "cooperative sociali", che sono tipologie organizzative differenti e distinte (che gestiscono in prima persona servizi socio-sanitari educativi, ed attività finalizzate all'inserimento lavorativo di particolari soggetti "svantaggiati"). Del resto, il fatto che le specifiche criticità organizzative e gestionali che una cooperativa è chiamata ad affrontare siano assolutamente diverse da quelle dei consorzi, è nella specie provato (cfr. pag. 271 e segg. dell’all. 2 al deposito di parte ricorrente del 21 ottobre 2003) dallo stesso Atto costitutivo del Consorzio ricorrente che, tra gli scopi sociali, elenca tutte attività di carattere strumentale e non direttamente operativo (es. stimolare la collaborazione tra le cooperative; realizzare l’inserimento di persone svantaggiate; formazione; commercializzazione dei prodotti, ecc.; informazione sociale; rapporti con il mondo imprenditoriale; promozione di nuove cooperative sociali; fornitura di beni e servizi ai soci; partecipazione agli appalti; ecc.). Come si vede le attività del Consorzio sono certamente connesse, ma sostanzialmente estranee alla produzione vera e propria dei beni e dei servizi delle cooperative sociali. In conclusione sul punto, il provvedimento appare del tutto esente dalle dedotte censure di eccesso di potere. 4. Deve infine essere disatteso il terzo motivo di gravame con cui il Consorzio ricorrente lamenta, che Sviluppo Italia avrebbe, erroneamente ed immotivatamente, ritenuto non garantito il rispetto della “operatività integrata delle iniziative”. Al riguardo la giurisprudenza ha costantemente affermato che, in materia di concessione di contributi economici, le valutazioni istruttorie effettuate su base tecnica, comportano scelte tipicamente discrezionali che, come tali, sono sindacabili in sede di legittimità solo per manifesti vizi logici, per errore di fatto, per travisamento dei presupposti, per difetto di istruttoria e, infine, per erronea applicazione delle regole tecniche (Cons. Stato, Sez. VI, 1 marzo 2002, n. 259). Ciò posto, la motivazione relativa all’assenza di un requisito essenziale espressamente previsto dall’art. 5 u.c., non poteva che essere ricognitiva di tale accertamento negativo. Al riguardo la parte ricorrente erroneamente assume che l’art. 5 introduceva un criterio che non consentiva a Sviluppo

Italia di valutare l'intensità o la qualità dell'integrazione operativa: al contrario Sviluppo Italia doveva puntualmente verificare non solo la completezza della documentazione e dei requisiti per l'ammissione alle agevolazioni ma doveva esercitare una valutazione discrezionale di merito sulla esistenza o meno del requisito della operatività integrata. In ogni caso la mancata indicazione, da parte dei promotori del progetto, degli elementi dai quali poter ricavare le utilità di scala connessa con l'operatività integrata non può essere supplita con il successivo apodittico, inconferente, e generico richiamo in questa sede al masterplan complessivo del progetto. Quindi neanche in ricorso, a dimostrazione dell'esattezza dell'assunto, la parte ricorrente ha introdotto riferimenti e particolari, in grado di dimostrare in base a quali elementi concreti potevano ravvisarsi i vantaggi e gli svantaggi derivanti dall'operatività integrata. Le censure, meramente formali del Consorzio ricorrente sul punto, sono del tutto inconsistenti ad inficiare, sul piano della logica e della razionalità, il provvedimento impugnato. 5. Il ricorso è infondato in tutti i suoi profili e deve in conclusione essere respinto. In relazione alla novità delle questioni può disporsi l'integrale compensazione delle spese del presente giudizio.

P.Q.M.

il Tribunale Amministrativo Regionale del Lazio – Sez. III^-ter : 1) respinge il ricorso di cui in epigrafe. 2) Spese compensate. Ordina che la presente sentenza sia eseguita dall'Autorità Amministrativa. Così deciso dal Tribunale Amministrativo Regionale del Lazio – Sez. III^-ter, in Roma, nella Camera di Consiglio del 13.11.2003.

IL PRESIDENTE dr. Francesco Corsaro
IL CONSIGLIERE-EST. dr. Umberto Realfonzo

CAPITOLO III

FIRMA DIGITALE

Il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) ha elaborato le "Linee guida per l'utilizzo della Firma Digitale" prendendo in esame l'argomento sia dal punto di vista giuridico legale, con particolare attenzione al valore probatorio della firma digitale e della firma elettronica , sia dal punto di vista dei possibili usi e sviluppi di un sistema di certificazione elettronica dei documenti.

Per quanto riguarda il primo aspetto oggetto dell'analisi è noto che a partire del 1997, una serie di provvedimenti legislativi hanno conferito valore giuridico al documento informatico e alla firma digitale. La pubblicazione della Direttiva Europea 1999/93/CE (Directive 1999/93/EC of the European Parliament and of the Council on a common framework for electronic signatures), nel gennaio del 2000, ha dato ulteriori impulsi al processo legislativo, imponendo un quadro comune agli Stati dell'Unione Europea.

La struttura normativa dettata dal legislatore comunitario ha introdotto differenti sottoscrizioni o, più correttamente, differenti livelli di sottoscrizione. Nel linguaggio corrente, quindi, hanno iniziato a essere utilizzati i termini firma "debole" o "leggera" e firma "forte" o "pesante".

Quest'ultimo tipo di firma, ovvero quella che il legislatore definisce firma digitale è basata su un sistema a chiavi crittografiche asimmetriche, utilizza un certificato digitale con particolari caratteristiche, rilasciato da un soggetto con specifiche capacità professionali garantite dallo Stato e viene creata mediante un dispositivo con elevate caratteristiche di sicurezza che in genere è una smart card.

L'altra tipologia di firma è la parte complementare. Tutto ciò che non risponde a quanto appena descritto ma è compatibile con la definizione giuridica di firma elettronica è un firma "leggera".

Dal punto di vista giuridico sono notevoli le differenze fra i due tipi di firma: la firma digitale è equivalente a una sottoscrizione autografa; le altre, invece, vengono valutate in fase di giudizio in base a caratteristiche oggettive di qualità e sicurezza.

Come ulteriore garanzia per la pubblica amministrazione, che è obbligata ad accettare i documenti firmati digitalmente, i certificatori che intendono rilasciare

certificati digitali validi per le sottoscrizioni di istanze e dichiarazioni inviate per via telematica alla pubblica amministrazione stessa, possono dimostrare di possedere particolari e comunque superiori caratteristiche di qualità e sicurezza e ottenere quindi la qualifica di "certificatore accreditato". Tale qualifica è sotto il controllo ed è garantita, in Italia, dallo Stato.

Dalle su indicate premesse appare evidente che per ottenere una sottoscrizione equivalente a quella autografa è indispensabile utilizzare la firma digitale, mentre negli altri casi non siamo in presenza di una vera e propria firma ma di un processo di autenticazione con minori requisiti di sicurezza e quindi con una minore efficacia probatoria.

Da quanto esposto inoltre si può dedurre che nella pubblica amministrazione l'espressione del potere di firma nel documento informatico da parte del funzionario che ne ha titolarità, dovrà essere esercitata con la firma digitale.

Per quanto concerne l'utilizzabilità della firma digitale le "linee guida per l'utilizzo della Firma Digitale" elaborate dal CNIPA sottolineano come questo tipo di firma è utile qualora sia necessario sottoscrivere una dichiarazione ottenendo la garanzia di integrità dei dati oggetto della sottoscrizione e di autenticità delle informazioni relative al sottoscrittore.

Esempi tipici dell'utilizzo della firma digitale possono essere ricercati in tutti gli adempimenti da effettuarsi verso le amministrazioni che richiedono appunto la sottoscrizione di una volontà: denunce, dichiarazioni di cambi di residenza, di domicilio, richieste di contributi, di esenzioni a pagamenti a causa del reddito o di altre condizioni particolari, ricorsi, ecc.

Fra privati può trovare un interessante impiego nella sottoscrizione di contratti, verbali di riunioni, ordini di acquisto, risposte a bandi di gara, ecc.

Peraltro la firma digitale trova già da tempo applicazione nel protocollo informatico, nella procedura di archiviazione documentale, nel mandato informatico di pagamento, nei servizi camerali, nelle procedure telematiche d'acquisto, ecc.

Per quanto riguarda la firma elettronica è necessario distinguere la firma elettronica (generica) che può essere realizzata con qualsiasi strumento (password, PIN, digitalizzazione della firma autografa, tecniche biometriche, ecc.) in grado di conferire un certo livello di autenticazione a dati elettronici dalla firma elettronica

avanzata, più sofisticata, che consente di identificare in modo univoco il firmatario garantendo anche l'evidenza di modifiche all'oggetto firmato, apportate dopo la sottoscrizione.

Allo stato dell'arte, solo il sistema a chiavi asimmetriche definito per la firma digitale nella legge italiana soddisfa i requisiti richiesti per la firma elettronica avanzata.

Dalle "Linee guida per l'utilizzo della Firma Digitale" si evince anche il grado di diffusione della firma digitale in Europa. Il F.E.S.A. (Forum of European Supervisor Authority), il cui scopo è far incontrare rappresentanti dei vari organismi di vigilanza nazionali in Europa per l'armonizzazione dei principi e delle tecniche fondamentali che regolano la materia nei rispettivi Stati, ha eseguito nell'ottobre 2002 una ricerca sulla diffusione della firma digitale da cui emerge che l'Italia era, con 500.000 certificati lo Stato con la maggiore diffusione di certificati, seguita dalla Norvegia con 32.000, e dalla Germania, con 26.000. Nel primo trimestre 2004 il numero dei dispositivi rilasciati in Italia per la firma digitale ha superato 1.250.000 unità.

Tuttavia sono emerse alcune problematiche giuridiche a seguito della diffusione della firma digitale in Europa in quanto la firma digitale, generata in qualunque Stato membro della Comunità deve, sulla base dei trattati comunitari, essere riconosciuta dagli altri Stati. Al fine di rendere agevole tale mutuo riconoscimento è indispensabile che le norme nazionali di recepimento della Direttiva europea 1999/93/CE sulle firme elettroniche nei rispettivi Stati, forniscano un insieme comune di garanzie e certezze.

In Italia la firma digitale ha trovato il riconoscimento legislativo necessario per il proprio utilizzo con la pubblicazione, in data 15 aprile 1999, delle regole tecniche costituite dal DPCM 8 febbraio 1999 (oggi sostituito dal DPCM 13 gennaio 2004).

In data 27 gennaio 2000 veniva incluso, nell'elenco pubblico dei certificatori, il primo soggetto autorizzato a rilasciare dispositivi di firma digitale utilizzabili per poter sottoscrivere documenti informatici con la medesima validità giuridica della firma autografa. Un richiamo ben preciso all'articolo 2702 del codice civile ne sanciva, infatti, la validità giuridica, prevedendo appunto che "La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta".

Quindi la firma digitale era giuridicamente valida, fatta salva la possibilità per il presunto sottoscrittore di disconoscerne la paternità. In tale evenienza era la controparte, e non il sottoscrittore, a doverne dimostrare la reale paternità.

Diversamente se una firma è "legalmente considerata come riconosciuta", ed è il caso, ad esempio, di una firma autenticata da un pubblico ufficiale, è il sottoscrittore che, per vederne nulli gli effetti, deve intentare una querela di falso.

Con il recepimento della Direttiva europea sulle firme elettroniche 1999/93/CE, il DLGS 23 gennaio 2002, n.10, modificando l'articolo 10 (L) " Forma ed efficacia del documento informatico" del DPR 28 dicembre 2000, n.445 (in cui era confluito il DPR 10 novembre 1997, n.513) rafforzava il valore giuridico di una sottoscrizione effettuata con firma digitale. Detto articolo, al comma 3, prescrive che "Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto ". Tale decreto legislativo è stato abrogato dall' articolo 75 del Codice dell'amministrazione digitale (d.lgs. 7 marzo 2005, n. 82, v. cap. VI) che dedica la sezione II (artt. 24-37) a "Firme elettroniche e certificatori".

Quindi, alla sottoscrizione con firma digitale "forte" viene data la medesima validità giuridica di una firma autografa autenticata da un pubblico ufficiale.

Invece per quanto riguarda le altre firme elettroniche il valore probatorio è inferiore; in un procedimento legale infatti tali firme elettroniche andranno analizzate di volta in volta dal giudice che deciderà se ammetterle quali prove in giudizio.

Tuttavia tale nuovo strumento ha notevoli potenzialità anche a livello amministrativo, in particolare per quanto concerne i rapporti fra cittadini e pubbliche amministrazioni nonché per la semplificazione delle attività delle stesse amministrazioni.

A tal proposito, nell'ambito dei lavori del Consiglio regionale del Piemonte si segnala il piano di attività 2005 elaborato congiuntamente dalla direzione Segreteria dell'Assemblea, dal settore Sistema informativo e Banca dati Arianna e dal CSI_Piemonte. In tale documento, approvato dall'Ufficio di Presidenza del Consiglio regionale, si individua una procedura – campione, nell'ambito di una direzione, su cui

avviare l'utilizzo della firma digitale. Tale sperimentazione si pone l'obiettivo di estendere l'utilizzo della firma digitale ad altre applicazioni fra cui l'invio di documenti da parte dei Consiglieri agli uffici (interpellanza, interrogazionei ecc.)

"Firmare europeo", un commento sulla direttiva 1999/93/Ce relativa ad un quadro comunitario per le firme elettroniche e sulla legislazione in materia in alcuni stati europei.

NUMERO SCHEDA: 6117

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: FIRMA DIGITALE

FONTE: LA NUOVA GIURISPRUDENZA CIVILE COMMENTATA

AUTORE: Giuliana Vangone

NUMERO: 6

DATA: 31/12/2004

PAGINA: 709-730

NATURA ATTO: COMMENTO

Si tratta di un articolo, a cura di Giuliana Vangone, intitolato "Firmare europeo", pubblicato sul numero 6/2004 (novembre-dicembre 2004) della rivista "La nuova giurisprudenza civile commentata".
In questo commento l'autrice analizza la direttiva 1999/93/Ce relativa ad un quadro comunitario per le firme elettroniche e la legislazione interna in materia di alcuni alcuni stati europei, dedicando l'ultimo capitolo ad un quadro comparativo.
Si riporta il sommario dell'articolo che è consultabile presso il settore Studi e documentazione legislativi.
1. Direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.
2. Austria: Legge Federale n. 190: Legge sulla firma elettronica - SigG, 1999 e Regolamento n. 30: Regolamento sulla firma elettronica - SigV.
3. Belgio: direttiva relativa alla firma elettronica emanata nel settembre 2001.
4. Francia: decreto n. 2001-272 del 30 marzo 2001 per l'applicazione dell'art. 1316-4 del codice civile e relativo alla firma elettronica.
5. Germania: legge regolante le condizioni strutturali per le firme elettroniche e rettificante altre regolamentazioni del 2001.
6. Irlanda: disegno di legge relativo al commercio elettronico 2000 riguardante le firme ed i certificati elettronici.
7. Regno Unito: norme relative alle firme elettroniche 2002 e note esplicative dell'Atto sulle comunicazioni elettroniche 2000.
8. Comparando.

Per il Tar Calabria il ricorso inviato per via telematica senza firma digitale è da considerarsi irricevibile.

NUMERO SCHEDA: 5948

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: FIRMA DIGITALE

FONTE: GIUSTIZIA AMMINISTRATIVA

RIFERIMENTO NORMATIVO: d.p.r. 445/2000

NATURA ATTO: SENTENZA

DATA ATTO: 09/02/2005

NUM.ATTO: 98

ORGANO: TAR CALABRIA

Con questa sentenza il tar della Calabria, sezione seconda di Catanzaro, ha affermato che il documento inviato tramite posta elettronica, ma non sottoscritto con la firma digitale o con un'altra tipologia di firma elettronica non possiede "*i requisiti legali necessari per ricondurne con certezza la paternità al ricorrente e, pertanto, detta trasmissione per via telematica non può essere considerata equivalente a quella di un documento formato per iscritto a mezzo posta ordinaria o corriere*". Il collegio osserva che il Testo unico in materia di documentazione amministrativa (d.p.r. n. 445/2000) pur ritenendo ammissibile la trasmissione del documento informatico per via telematica, prevede che lo stesso soddisfa il requisito legale della forma scritta solamente se sottoscritto con firma digitale o con altra tipologia di firma elettronica avanzata.
Nel caso di specie il Tar ha ritenuto irricevibile un ricorso gerarchico trasmesso per posta elettronica ma privo di firma digitale.

Si allega il testo della sentenza.

Si segnala inoltre un'interessante commento alla sentenza sulla rivista "D & G, diritto e giustizia", n. 11 del 19 marzo 2005, consultabile presso il settore Studi e documentazione legislativi.
L'articolo, a cura di Michele Iaselli, si intitola "Sì all'*e-mail*, ma solo se è autenticata. Paternità incerta senza firma digitale. Dottrina divisa sui requisiti per l'equivalenza agli atti cartacei".
Il commento, ricco di riferimenti legislativi, giurisprudenziali e dottrinali, dopo una breve premessa nella quale si evidenzia come la questione affrontata dal Tar Calabria riprenda una questione particolarmente discussa negli ambienti giuridici, si sofferma sulle seguenti tematiche:
- "Messaggi di posta elettronica: il valore giuridico".
- "Documenti informatici ed efficacia probatoria".
- "Regole confuse, il legislatore fa piazza pulita".
"La certificazione di invio e ricezione".

Si allega il testo integrale della sentenza.

FATTO

Il ricorrente, maresciallo capo della stazione Carabinieri di Gizzeria Lido, con nota prot. 385/1 del 15.11.2003, a firma del Comandante della Compagnia Carabinieri di Lamezia Terme, riceveva comunicazione dell'avvio di un procedimento disciplinare nei suoi confronti, perché, in data 9.11.2003, "ometteva di dare comunicazione alla centrale operativa di essere impossibilitato ad intraprendere il servizio poiché affetto da una momentanea indisposizione fisica".
Dopo la presentazione di memoria difensiva in data 28.11.2003, al ricorrente veniva comminata la sanzione disciplinare di giorni tre di consegna, con provvedimento del Comandante della Compagnia di Lamezia Terme, comunicatogli il 30.01.2004.
Avverso tale sanzione disciplinare, il ricorrente proponeva ricorso gerarchico al Comandante Provinciale dei Carabinieri di Catanzaro, inoltrandolo mediante posta elettronica il 1°.03.2004. Tale ricorso veniva inoltre trasmesso in originale, su supporto cartaceo, a mezzo corriere, al Comando Provinciale il 2.03.2004 (data di avvenuta ricezione).
Con il provvedimento oggetto di presente gravame, il ricorso veniva dichiarato irricevibile, in quanto proposto oltre il termine di trenta giorni dalla notifica del provvedimento disciplinare.
Avverso detto provvedimento, il ricorrente ha articolato un triplice ordine di motivi, contestando la dichiarazione di irricevibilità e riproponendo censure attinenti al merito del provvedimento applicativo della sanzione disciplinare inflittagli.
Con la memoria di costituzione in giudizio, l'Amministrazione intimata ha chiesto il rigetto del proposto gravame.
All'udienza del 3 dicembre 2004, sentiti i difensori delle parti come da relativo verbale, il ricorso veniva trattenuto in decisione.

DIRITTO

1. Il ricorso è inammissibile per le ragioni di seguito esplicitate.
2. Con il primo motivo, è stata invero contestata la declaratoria di irricevibilità del ricorso gerarchico proposto dal ricorrente, in quanto l'Amministrazione resistente non avrebbe considerato che la trasmissione a mezzo posta elettronica deve considerarsi equivalente agli altri mezzi di trasmissione previsti dalla legge.
Il motivo si appalesa privo di pregio.
Risulta per tabulas che la trasmissione mediante posta elettronica avvenne il 1°.03.2004, alle ore 22.06, mentre la presentazione del ricorso su supporto cartaceo presso gli Uffici della Compagnia di Lamezia Terme avvenne il giorno successivo. Del pari documentalmente provato è che il provvedimento applicativo della sanzione disciplinare venne comunicato al ricorrente il 30.01.2004.
Per effetto della disposizione dell'art. 2, 1° comma, l. n. 1199/71, il ricorso gerarchico deve essere presentato nel termine di trenta giorni dalla data della notificazione o della comunicazione in via amministrativa dell'atto impugnato; il comma successivo precisa che tale ricorso può essere inoltrato "direttamente o mediante lettera raccomandata con avviso di ricevimento" e che allorquando sia inoltrato a mezzo posta, "la data di spedizione vale quale data di presentazione".
Nel caso di specie, il ricorso non fu inoltrato a mezzo posta ordinaria, bensì mediante utilizzo dello strumento telematico della posta elettronica e, di seguito, mediante corriere.
Il mancato utilizzo dello strumento della posta ordinaria, segnatamente della lettera raccomandata a.r., rende chiaramente inapplicabile la disposizione normativa secondo cui "la data di spedizione vale quale data di presentazione".
Facendo applicazione in subiecta materia della disciplina generale sul computo dei termini contenuta nell'art. 155 c.p.c., ne discende, inoltre, che per essere tempestivo il ricorso gerarchico avrebbe dovuto essere presentato il 1°.03.2004, giacché il termine di trenta giorni, decorrente dal 30.01.2004 (data di comunicazione del provvedimento disciplinare), non computando il dies a quo e tenendo conto del fatto che il 29.02.2004 era giorno festivo, scadeva proprio in tale data.
Secondo l'approccio prescelto dal ricorrente, poiché la trasmissione a mezzo posta elettronica deve essere considerata equivalente alla presentazione personale, il ricorso sarebbe stato nel caso di specie tempestivo.
Tale approccio non può essere condiviso dal Collegio, giacché non conforme alla disciplina contenuta nel vigente Testo unico in materia di documentazione amministrativa (D.P.R. 28 dicembre 2000, n. 445). Ed invero, sebbene l'art. 14, 1° comma, stabilisca che "Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato", e l'art. 1, lett. b) definisca documento informatico "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", tale disciplina non è nella specie applicabile in quanto il ricorso

gerarchico inoltrato per via telematica non era accompagnato da firma digitale o altra tipologia di firma elettronica. Detta mancanza, rende difatti inapplicabili le previsioni normative dell'art. 10, 2° e 3° comma, del Testo unico, secondo le quali, rispettivamente, "il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta" e "quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto".
Ne discende che il documento inviato mediante posta elettronica il 1°.03.2004, alle ore 22.06, non essendo stato sottoscritto con firma digitale o altra tipologia di firma elettronica, non possedeva i requisiti legali necessari per ricondurne con certezza la paternità al ricorrente e, pertanto, detta trasmissione per via telematica non può essere considerata equivalente a quella di un documento formato per iscritto a mezzo posta ordinaria o corriere.
L'impossibilità di ritenere rituale detta proposizione del ricorso gerarchico, impone al Collegio la conclusione che il ricorso in questione fu presentato ritualmente, sebbene tardivamente, soltanto il 2.03.2004, allorquando, a mezzo corriere, pervenne al Comando Compagnia di Lamezia Terme ed ivi fu assunto al protocollo n. 183/1 (v. attestazione in atti, a firma del Capitano Paolo Storoni).
Per le ragioni sin qui esposte, la declaratoria di irricevibilità per tardività di cui al provvedimento oggetto di gravame, sfugge alle censure proposte dal ricorrente.
3. Da tale ultima conclusione discende quella della inammissibilità del ricorso giurisdizionale in epigrafe, e ciò in ossequio all'art. 16, 2° comma, della legge 1° luglio 1978, n. 382 ("Norme di principio sulla disciplina militare).
Secondo la norma citata, avverso le sanzioni disciplinari di corpo non è ammesso il ricorso giurisdizionale o straordinario, se prima non sia stato esperito il ricorso gerarchico o siano trascorsi novanta giorni dalla data di presentazione del ricorso. La Corte Costituzionale (C. Cost. 22 aprile 1997, n. 113), scrutinando talune censure di incostituzionalità sollevate all'insegna della norma, ha chiarito che è pienamente conforme alla Carta fondamentale ed a una ponderata considerazione, da un lato, dell'ordinamento gerarchico militare, dall'altro del diritto di difesa costituzionalmente garantito, la previsione legislativa della necessità per il militare di previa impugnazione in via amministrativa del provvedimento disciplinare, ove intenda percorrere la strada della tutela davanti ad organi giurisdizionali dello Stato.
Nel caso di specie, il ricorrente non ha adempiuto all'onere previsto dall'art. 16, 2° comma, l. n. 382/78, giacché il ricorso gerarchico, come già evidenziato, è stato proposto tardivamente. Né si può ritenere che la tardiva proposizione sia comunque sufficiente per soddisfare il requisito normativo della previa proposizione del ricorso gerarchico, in quanto tale ultima interpretazione svuoterebbe di qualsiasi contenuto la norma legislativa, la cui ratio è di postergare, nel rispetto della gerarchia propria dell'ordinamento militare, l'intervento giurisdizionale rispetto al pronunciamento degli organi interni del corpo. Poiché un ricorso gerarchico tardivo deve essere dichiarato irricevibile, la ratio legislativa verrebbe chiaramente elusa.
Si impone, pertanto, la declaratoria di inammissibilità del ricorso giurisdizionale in epigrafe.
4. La natura delle questioni esaminate configura comunque giusto motivo per compensare integralmente tra le parti spese, diritti ed onorari di giudizio

P.Q.M.

Il Tribunale Amministrativo Regionale per la Calabria – Sezione Seconda definitivamente pronunziando sul ricorso in epigrafe, lo dichiara inammissibile.
Compensa spese, diritti ed onorari di giudizio.
Ordina che la presente sentenza venga eseguita dall'Autorità Amministrativa.
Così deciso in Catanzaro nella Camera di Consiglio del 3 dicembre 2004.

Pubblicate in G.U. le Linee guida in materia di digitalizzazione dell'amministrazione.

NUMERO SCHEDA: 5947

CLASSIFICAZIONE: E-GOVERNMENT

FONTE: ITALIA OGGI

NATURA ATTO: DIRETTIVA

DATA ATTO: 04/01/2005

ORGANO: MINISTERI

Sono state pubblicate sulla Gazzetta ufficiale n. 35 del 12 febbraio 2005 le "Linee guida in materia di digitalizzazione dell'amministrazione" ,contenute nella direttiva del 4 gennaio 2005 emanata dal Ministro per l'innovazione e le tecnologie.
Tale direttiva si prefigge di fornire le necessarie indicazioni per la concreta realizzazione dell'obiettivo della digitalizzazione della p.a., al fine di favorire un impiego più efficiente e razionale delle risorse umane e finanziarie e allo scopo di eliminare le disomogeneità attualmente riscontrabili in questo ambito fra le diverse amministrazioni.
In particolare, le Linee guida, nell'evidenziare gli apprezzabili risultati già conseguiti, individuano le criticità da risolvere e i traguardi ancora da raggiungere. Fra questi ultimi si segnalano:

- la disponibilità on-line di un numero sempre maggiore di servizi prioritari;
- l'estensione dell'utilizzo della firma digitale;
- l'ampliamento dell'impiego della posta elettronica;
- l'ulteriore diffusione delle competenze informatiche acquisite dal personale;
- lo sviluppo dell'accesso on-line all'iter delle pratiche, mediante diffusione del protocollo informatizzato, prerequisito della trasparenza amministrativa, e dei call center, utilizzabili anche per verificare lo stato delle pratiche e per la risoluzione dei problemi connessi;
- la dotazione dei necessari strumenti di rilevazione della soddisfazione degli utenti, non ancora presenti in tutti gli uffici.
- Proprio allo scopo di rimediare alle carenze rilevate, ogni Amministrazione dovrà verificare al proprio interno lo stato di attuazione degli obiettivi di legislatura e le ragioni dell'eventuale ritardo, predisponendo un piano di recupero che ne consenta il perseguimento nei tempi stabiliti.

Le Linee guida considerano conclusa la prima fase della digitalizzazione della p.a., contraddistinta dalla definizione di un nuovo quadro normativo e dallo sviluppo delle infrastrutture di base, dalla diffusione di conoscenze informatiche tra i dipendenti, dall'attivazione sia di siti web quali canali di informazione e talora di erogazione di servizi on line agli utenti sia di singoli strumenti e specifici istituti, quali la firma digitale, il protocollo informatico, la posta elettronica certificata, la Carta di identità elettronica e la Carta Nazionale dei Servizi.
La seconda fase, il cui presupposto normativo risiede nelle due riforme organiche che costituiscono la base per il futuro sviluppo dell'e-Government (il Sistema Pubblico di Connettività e Cooperazione, destinata a sostituire la Rete Unitaria delle Pubbliche Amministrazioni, e il Codice dell'Amministrazione digitale), produrrà la "dematerializzazione dei documenti" nonché forme di "interazione a distanza, di circolarità e standardizzazione dei dati, di multicanalità, di accessibilità, di nuove

competenze professionali". In pratica, la digitalizzazione della p.a. consentirà ai cittadini di interagire con qualunque amministrazione attraverso la rete a fronte di un imponente sforzo organizzativo di tutte le p.a. per rendere sempre disponibili tutte le informazioni in modalità digitale.
Le Linee guida passano poi a illustrare le aree di intervento per l'effettiva realizzazione del progetto di digitalizzazione della p.a.. Ad essere interessati sono i settori della comunicazione elettronica, della Rete Internazionale delle pubbliche amministrazioni, del sistema pubblico di connettività e cooperazione, della Carta Nazionale dei Servizi, dei servizi on line agli utenti e della gestione documentale.
Con riguardo all'aspetto finanziario, le Linee guida rinviano a successivi DPCM la predisposizione di un programma strutturale per l'informatica pubblica volta a razionalizzarne i costi senza comprimerne l'impulso all'innovazione e allo sviluppo di soluzioni tecnologiche e organizzative innovative. Per evitare che tale sviluppo produca un incremento della spesa informatica e nell'intento di conseguire economie gestionali, le Linee guida suggeriscono l'adozione di precise modalità di approvvigionamento dei servizi, un'attiva collaborazione con il CNIPA e l'impiego della tecnologia "Voice over IP", che consente il trasferimento delle conversazioni vocali mediante server di rete in luogo di centrali telefoniche e centralini. L'adozione di questa tecnologia consente di ricorrere ad un collegamento unico per qualsiasi tipo di comunicazione (voce, dati e immagini) attraverso il Sistema Pubblico di Connettività e la Rete Internazionale delle Pubbliche Amministrazioni, con indubbi vantaggi, a parità di qualità del servizio, per i costi di telefonia, gestione e manutenzione.
Infine, le Linee guida attribuiscono un ruolo determinante per la riuscita della digitalizzazione della p.a. al coinvolgimento dei dirigenti, ai quali dovranno essere assegnati idonei obiettivi da realizzare nel corso del 2005.

Si segnala un commento alla direttiva sulla rivista "Guida agli Enti Locali", n. 14 del 9 aprile 2005, pp. 58-60, a cura di P. Subioli, consultabile presso il settore Studi e documentazione legislativi.
Si allega altresì il testo della direttiva.

Direttiva del 4 gennaio 2005
LINEE GUIDA IN MATERIA DI DIGITALIZZAZIONE DELL'AMMINISTRAZIONE
PREMESSA
La presente direttiva è indirizzata a tutte le Amministrazioni dello Stato e a tutti gli Enti pubblici sottoposti a vigilanza ministeriale. Per le Regioni e gli Enti locali costituisce contributo alle determinazioni in materia, nel rispetto della loro autonomia amministrativa, e sarà oggetto di successivo atto di indirizzo ai sensi dell'articolo 29, comma 7, della legge 23 dicembre 2001, n. 448 (legge finanziaria per il 2002). Può rappresentare schema di riferimento anche per le altre amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165. Le precedenti direttive 1 e gli altri atti di indirizzo in materia di digitalizzazione, emanati anche in relazione a specifici settori, devono, comunque, intendersi validi ed efficaci e costituiscono parte integrante delle seguenti disposizioni.
1. STATO DI ATTUAZIONE DEGLI OBIETTIVI DI DIGITALIZZAZIONE 2
La rilevazione sullo stato di attuazione degli obiettivi di legislatura nella pubblica amministrazione ha evidenziato il raggiungimento di significativi risultati. Permangono, peraltro, disomogeneità tra le diverse amministrazioni.
In particolare si segnalano di seguito i principali risultati conseguiti e le maggiori criticità da affrontare:
a) circa il 50% dei servizi prioritari sono disponibili on-line, altri sono disponibili solo parzialmente. Per quelli rispetto ai quali si registrano criticità le Amministrazioni dovranno effettuare un'analisi puntuale

dei motivi di ritardo, e produrre un piano al fine di accelerarne la realizzazione. E' in ogni caso opportuno attivare la verifica della soddisfazione dell'utente;
1Direttiva del 21 dicembre 2001, pubblicata in Gazzetta Ufficiale del 5 febbraio 2002 n. 30; Direttiva del 20 dicembre 2002, pubblicata in Gazzetta Ufficiale del 4 marzo 2003 n. 52 Direttiva del 18 dicembre 2003, pubblicata in Gazzetta Ufficiale del 4 febbraio 2004 n. 28
2OBIETTIVI DI DIGITALIZZAZIONE PER LA LEGISLATURA indicati nelle "Linee guida del Governo per lo sviluppo della Società dell'Informazione" pubblicate sul sito www.innovazione.gov.it:
Servizi online ai cittadini e alle imprese
1. Tutti i servizi "prioritari" disponibili on-line
2. 30 milioni di Carte di Identità Elettroniche e Carte Nazionali dei Servizi distribuite
3. 1 milione di firme digitali diffuse entro il 2003
Efficienza interna della Pubblica Amministrazione
4. 50% della spesa per beni e servizi tramite eProcurement
5. Tutta la posta interna alla Pubblica Amministrazione via e-mail
6. Tutti gli impegni e mandati di pagamento gestiti on-line
Valorizzazione delle Risorse Umane
7. Alfabetizzazione certificata di tutti i dipendenti pubblici eleggibili
8. 1/3 della formazione erogata via eLearning
Trasparenza
9. 2/3 degli uffici della Pubblica Amministrazione con accesso on-line all'iter delle pratiche da parte dei cittadini
Qualità
10. Tutti gli uffici che erogano servizi dotati di un sistema di soddisfazione dell'utente.

b) sono state distribuite oltre 1,6 milioni di carte di firma digitale. Il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA) ha distribuito oltre 23.000 smart card ad altrettanti funzionari pubblici, con le quali vengono firmati digitalmente ogni giorno circa 3.000 mandati di pagamento. E' necessario rivedere le procedure amministrative al fine di estendere rapidamente l'utilizzo della firma digitale;
c) l'utilizzo della posta elettronica è sensibilmente aumentato nelle comunicazioni interne alla Pubblica Amministrazione. Poiché il completamento dell'Indice PA (elenco di tutti gli uffici pubblici con casella di posta elettronica a disposizione del pubblico), attualmente in corso di predisposizione ad opera del CNIPA, costituirà certamente un incentivo all'uso di tale strumento, si invitano le Amministrazioni che non abbiano ancora ottemperato all'invio dei dati ad attivarsi in tal senso con la massima urgenza garantendo, altresì, il tempestivo e costante aggiornamento dei dati stessi;
d) sempre nel settore della posta elettronica, va segnalato che molte amministrazioni hanno avviato iniziative per accrescere l'efficienza e ridurre i costi di proprie attività sostituendo ad operazioni materiali il ricorso a comunicazioni elettroniche. In questo ambito si colloca anche l'iniziativa denominata @P@3, finalizzata a cofinanziare specifici progetti delle Amministrazioni. E' allo studio la possibilità di rilanciare il progetto per ulteriori iniziative di razionalizzazione e risparmi;
e) attualmente 25 milioni di impegni e mandati di pagamento sono on line. Nel corso del 2004 si è, infatti, esteso l'uso del Sicoge a quasi tutte le amministrazioni centrali (coprendo quasi il 100% dei capitoli di spesa delle stesse). Inoltre è stata automatizzata anche la gestione degli ordini di accreditamento che, a partire da giugno, comporta la gestione telematica di circa 175 mila ordini di accreditamento annuali; occorre però ancora estendere tali sistemi alle contabilità speciali;
f) le competenze informatiche acquisite dal personale pubblico sono molto diffuse; i dati sulla formazione a distanza (e-learning) indicano una crescita superiore al 60% sebbene permanga poco rilevante il numero delle certificazioni tipo ECDL o equivalenti;
g) l'accesso on-line all'iter delle pratiche mostra difficoltà legate al notevole impatto organizzativo. E' comunque in crescita la diffusione del protocollo informatizzato, prerequisito della trasparenza amministrativa. Nei settori nei quali è maggiore l'esigenza dei cittadini, ad es. fisco e previdenza, sono pienamente operativi call center utilizzabili anche per verificare lo stato delle pratiche e risolvere i problemi connessi. Per le Amministrazioni che non abbiano ancora completato l'automazione della gestione documentale e del protocollo informatico si segnala che il CNIPA propone tale servizio in modalità ASP 4;
h) non sono ancora presenti in tutti gli uffici i necessari strumenti di rilevazione della soddisfazione degli utenti.

3 Progetto approvato dal Comitato dei Ministri per la Società dell'Informazione il 18 marzo 2003 pubblicato sul sito www.cnipa.gov.it.
4 ASP (Application Service Provider): servizi resi disponibili in rete per le amministrazioni, le quali possono acquisirli senza dover sviluppare soluzioni proprie e senza acquistare hardware e licenze software.
Azioni conseguenti – Piani di recupero
Ogni Amministrazione dovrà verificare al proprio interno lo stato di attuazione degli obiettivi di legislatura, i motivi del mancato o parziale raggiungimento, e predisporre un Piano di recupero che ne consenta il conseguimento nei tempi stabiliti. Detti Piani di recupero costituiranno parte integrante del Piano esecutivo per le tecnologie dell'informazione e della comunicazione (ICT) per il 2005 da trasmettere al CNIPA entro il 31 gennaio del 2005, redatto secondo le modalità stabilite al punto 6 della direttiva del 18 dicembre 2003.

2. LA SECONDA FASE DELLA DIGITALIZZAZIONE DELLA P.A.
Gli anni 2001-2004 hanno rappresentato la prima fase della digitalizzazione della Pubblica Amministrazione, nella quale l'impegno del Governo e delle amministrazioni è stato rivolto, soprattutto, al riorientamento ai servizi, allo sviluppo delle infrastrutture di base, alla diffusione di competenze informatiche e di una crescente familiarità con gli strumenti informatici tra i dipendenti e, nel periodo più recente, all' attivazione di siti web come canali di informazione ed in alcuni casi di erogazione di servizi on line agli utenti. In questa fase si è, quindi, pervenuti ad una maggiore diffusione, negli uffici e nei processi di lavoro, dell'uso delle ICT. Le basi di questo importante processo di crescita sono state consapevolmente tracciate non solo e non tanto in disposizioni legislative, quanto – piuttosto – innescando un circuito virtuoso "definizione di obiettivi – attuazione – controllo" nelle amministrazioni, sostenuto anche attraverso il cofinanziamento di iniziative di innovazione proposte dalle stesse amministrazioni, sia centrali (attraverso deliberazioni del Comitato dei Ministri per la Società dell'Informazione) che locali (programma di e-Government). Nel frattempo, come noto, sono stati disciplinati singoli strumenti e specifici istituti che connotano la digitalizzazione dell'Amministrazione (firma digitale, protocollo informatico, posta elettronica certificata, Carta di identità elettronica e Carta Nazionale dei Servizi, ecc.). Questa prima importante fase della digitalizzazione della Pubblica Amministrazione può essere considerata conclusa. Infatti, sulla base del patrimonio di esperienze maturate, ha preso corpo la definizione di una nuova cornice normativa, che induce le amministrazioni a non adottare gli strumenti offerti dalle tecnologie dell'informazione e della comunicazione quali "possibilità aggiuntive" dell'azione amministrativa, ma a sostituire gli strumenti e le modalità tradizionali di rapporto con gli utenti e di svolgimento delle attività interne.
E' ora il momento di attivare la seconda fase, che dovrà essere improntata alla piena valorizzazione degli investimenti già realizzati, alla razionalizzazione del sistema nel suo complesso, alla interoperabilità tra le amministrazioni, alla effettiva ed ampia transizione verso modalità di erogazione dei servizi on line e, infine, al raccordo pieno tra digitalizzazione, organizzazione, processi e servizi al pubblico. Questo passaggio dalla prima alla seconda fase della digitalizzazione trova la sua cornice normativa nell'approvazione di due riforme organiche che costituiranno la base per l'evoluzione dell'e-Government nei prossimi anni. La prima riforma è contenuta nel decreto legislativo sul Sistema Pubblico di Connettività e Cooperazione, ormai vicino alla definitiva adozione e che sostituirà, nello spirito di una visione pienamente condivisa tra Stato, Regioni ed Enti Locali, la Rete Unitaria delle Pubbliche Amministrazioni. Il nuovo sistema raccorderà tutte le pubbliche amministrazioni statali, regionali e locali. La seconda riforma è costituita dal "Codice dell'Amministrazione digitale"5, che darà un assetto unitario ed organico al complesso di diritti dei cittadini e delle imprese, agli istituti giuridici ed ai doveri delle amministrazioni in materia di digitalizzazione delle pubbliche amministrazioni. La prossima approvazione del decreto legislativo costituisce l'inizio di una seconda fase della digitalizzazione delle pubbliche amministrazioni, in quanto rende obbligatoria l'innovazione nella Pubblica Amministrazione nel modo più naturale: da una parte dando ai cittadini il diritto di interagire sempre, ovunque e verso qualunque amministrazione attraverso la rete; dall'altra, stabilendo che tutte le amministrazioni devono organizzarsi in modo da rendere sempre e comunque disponibili tutte le informazioni in modalità digitale.
Nuovi principi
I decreti legislativi concernenti il Sistema Pubblico di Connettività e Cooperazione (SPC) e il Codice dell'Amministrazione digitale forniranno l'adeguato supporto normativo in materia di dematerializzazione dei documenti, di comunicazione elettronica, di interazione a distanza, di

circolarità e standardizzazione dei dati, di multicanalità, di accessibilità, di nuove competenze professionali. In relazione a tali nuovi principi, le Amministrazioni pubbliche, anche con il supporto del CNIPA, dovranno, nel corso dell'anno 2005, porre in essere tutte le azioni di competenza per cogliere appieno le opportunità offerte dai nuovi strumenti. In tale contesto, sarà necessario perseguire una piena integrazione degli interventi di digitalizzazione con le politiche di riforma delle pubbliche amministrazioni, con specifico riferimento alla semplificazione delle procedure e dell'organizzazione amministrativa ed alla formazione del personale. In particolare, le amministrazioni, nel programmare i loro interventi di digitalizzazione, dovranno segnalare al Dipartimento della funzione pubblica ed al Ministro per l'innovazione e le tecnologie sia le opportunità/necessità di semplificazione dei procedimenti amministrativi e delle regolamentazioni interne, sia i fabbisogni di nuove competenze, ai fini della adozione degli interventi conseguenti.

5

Lo schema di decreto legislativo, recante il Codice dell'Amministrazione digitale, è stato approvato in via preliminare dal Consiglio dei Ministri in data 11 novembre 2004

Settori di intervento

Le seguenti aree costituiscono settori di intervento essenziali alla realizzazione della seconda fase della digitalizzazione. Essi richiedono uno sforzo sinergico da parte delle singole Amministrazioni al fine di dare esecuzione alle azioni previste dalla normativa vigente e per la realizzazione delle quali il CNIPA ha impegnato le proprie risorse ed avviato le necessarie attività progettuali:

Comunicazione elettronica

Nel rammentare la direttiva concernente l'impiego della posta elettronica nelle pubbliche amministrazioni6, nonché le norme relative all'utilizzo della firma digitale, si fa presente che sono di prossima definitiva approvazione le disposizioni necessarie per assicurare piena validità giuridica alle comunicazioni per via elettronica7, sia all'interno di ciascuna amministrazione, sia tra amministrazioni diverse, sia, infine, tra amministrazioni, cittadini e imprese. Di conseguenza diviene necessario riorganizzare il lavoro all'interno delle amministrazioni per sviluppare l'uso degli strumenti telematici, sostenendo minori oneri per la spedizione e l'archiviazione con notevoli vantaggi di velocità dell'azione amministrativa.

Rete Internazionale delle pubbliche amministrazioni

Per avvalersi dei previsti finanziamenti del CNIPA, le Amministrazioni che necessitano di connettività internazionale dovranno sottoscrivere i contratti di fornitura con l'aggiudicatario entro il primo trimestre del 2005.

Sistema Pubblico di Connettività e Cooperazione

Nelle more dell' attuazione del nuovo sistema, le Amministrazioni dovranno pianificare la migrazione dalla Rete Unitaria verso il nuovo Sistema Pubblico di Connettività e Cooperazione (SPC) presentando al CNIPA i relativi piani entro il 2005, al fine di non superare il termine di sei mesi dalla data del contratto quadro che sarà stipulato dal CNIPA.

6 Direttiva del 27 novembre 2003 pubblicata in Gazzetta Ufficiale del 12 gennaio 2004 n. 8 7 Schema di DPR sull'utilizzo della Posta Elettronica Certificata (PEC) approvato in via preliminare dal Consiglio dei Ministri del 25 marzo 2004

Carta Nazionale dei Servizi (CNS)

Sono ormai definite con decreto dei Ministri dell'Interno, per l'innovazione e tecnologie, dell'economia e delle finanze, datato 9 dicembre 2004, 8 le regole tecniche sulla CNS; le amministrazioni dovranno, pertanto, programmare l'emissione della CNS in sostituzione di altri strumenti di accesso ai servizi sino ad ora realizzati, tenendo comunque presente che, ai sensi della normativa vigente, ogni Amministrazione deve, comunque, garantire l'accesso ai propri servizi da parte dei titolari di CNS. Al fine di promuoverne la diffusione il CNIPA definirà un contratto quadro per la fornitura di CNS al quale le pubbliche amministrazioni potranno aderire.

Servizi on line agli utenti

Si conferma la priorità di favorire la diffusione e l'utilizzo di servizi on line per cittadini ed imprese, per migliorare il servizio e ridurre i costi. Le amministrazioni dovranno, pertanto, curare la realizzazione e la promozione di servizi interattivi, assicurando, nel contempo, la possibilità di accesso attraverso una pluralità di canali (internet, telefonia mobile, telefonia fissa, tv digitale), ciascuno facoltativamente fruibile dagli utenti. In tale ottica le amministrazioni dovranno collaborare per integrare i procedimenti di rispettiva competenza, al fine di agevolare gli adempimenti richiesti alle imprese e accrescere l'efficienza nelle aree che coinvolgono più amministrazioni, attraverso la definizione e l'attuazione di

accordi per la partecipazione al sistema di cooperazione attuato nell'ambito del Sistema per i servizi integrati alle imprese (www.impresa.gov.it).

Gestione documentale

Le amministrazioni dovranno porre in atto tutte le misure previste dalla normativa in materia di gestione documentale eventualmente avvalendosi dei servizi resi disponibili dal CNIPA nell'ambito dell'iniziativa Servizio di gestione del Protocollo Informatico e gestione documentale in modalità ASP.

3. RISPARMI e RAZIONALIZZAZIONE

L'articolo 1, commi da 192 a 196, della legge finanziaria per il 2005, introduce nuovi modelli di comportamento per le pubbliche amministrazioni finalizzati alla razionalizzazione dei processi operativi e, conseguentemente, al contenimento della spesa. La sua attuazione avverrà attraverso l'emanazione di successivi DPCM che individueranno le aree prioritarie e l'ambito soggettivo di intervento, al fine di predisporre un programma strutturale per l'informatica pubblica e la sua contestuale razionalizzazione, mantenendo l'attuale impulso all'innovazione, accelerando lo sviluppo e la diffusione di soluzioni tecnologiche e organizzative innovative, evitando, altresì, che questo sviluppo si traduca in incremento della spesa informatica e, al contrario, producendo economie. Ciò sarà possibile utilizzando le nuove modalità di approvvigionamento dei servizi che semplificano le incombenze delle singole amministrazioni, anche assumendo come modello di riferimento quello dei servizi ASP. Per la migliore attuazione della nuova disciplina introdotta dalla legge finanziaria è auspicabile un'attiva collaborazione con il CNIPA da parte delle Amministrazioni che potranno contribuire a determinarne gli ambiti di azione, effettuando una accurata analisi della propria situazione in rapporto all'utilizzo delle ICT al fine di individuare: -i casi di duplicazione o ridondanza di sistemi e strutture informatiche, sui quali sia possibile intervenire per razionalizzare e conseguire economie gestionali; -i casi in cui sia possibile ed opportuno utilizzare soluzioni condivise o soluzioni già adottate in altre amministrazioni. E' da sottolineare la possibilità di conseguire economie anche attraverso l'applicazione della Direttiva inerente l'acquisizione del software9, da effettuarsi attraverso una valutazione comparativa che tenga anche conto di prodotti disponibili in riuso od a codice sorgente aperto. E' all'uopo disponibile una proposta di metodologia di valutazione messa a punto dal CNIPA. Nell'ambito delle iniziative tendenti alla razionalizzazione ed al risparmio, particolare importanza assume l'adozione della tecnologia "Voice over IP", che consente di trasportare le conversazioni vocali via Internet o su reti per trasmissione dati che operano in modo analogo ad Internet, impiegando router e server di rete in luogo di centrali telefoniche e centralini. I centralini, pertanto, vengono sostituiti da server, utilizzando, di norma, il cablaggio esistente ed eliminando così costose duplicazioni. L'adozione di questa tecnologia consente di ricorrere ad un collegamento unico per qualsiasi tipo di comunicazione (voce, dati e immagini), attraverso il Sistema Pubblico di Connettività e la Rete Internazionale delle Pubbliche Amministrazioni, che sono state progettate per un trasporto di qualità per ciascuna delle indicate tipologie di comunicazioni. I vantaggi concreti potenzialmente derivanti dall'adozione del Voip consistono in una notevole riduzione delle spese di telefonia, oltre che delle spese di gestione e manutenzione, a parità di qualità del servizio, grazie :

-all'azzeramento dei costi delle conversazioni all'interno delle amministrazioni nonché alla riduzione dei costi delle chiamate verso l'esterno; -alla riduzione dei costi di gestione per l'impiego di un unico cablaggio e di impianti della stessa tipologia per voce e dati; -all'azzeramento dei costi legati agli spostamenti delle connessioni telefoniche del personale che possono essere realizzati con un semplice comando via software. Le Pubbliche Amministrazioni con contratti in scadenza a breve in questo settore dovranno valutare, prima del rinnovo dei contratti stessi, la convenienza del passaggio alle nuove tecnologie, anche avvalendosi dell'apposito Centro di Competenza, all'uopo istituito presso il CNIPA che potrà fornire, anche, supporto alla pianificazione dell'introduzione della tecnologia Voip ed alla sostituzione degli impianti esistenti, da programmare nell'arco di tre anni.

8 Decreto pubblicato sui siti: www.innovazione.gov.it e www.cnipa.gov.it.

9 Direttiva del 19 dicembre 2003 "Sviluppo ed utilizzazione dei programmi informatici da parte delle pubbliche amministrazioni" pubblicata in Gazzetta Ufficiale del 7 febbraio 2004 n. 31

4. RUOLO DELLA DIRIGENZA

Per la realizzazione dei citati obiettivi e per il successo della seconda fase di digitalizzazione dell'Amministrazione, appare necessario il più ampio coinvolgimento dei dirigenti ai quali dovranno essere, conseguentemente, assegnati corrispondenti obiettivi da realizzare nel corso dell'anno. Tale coinvolgimento dovrà mirare ad ottenere, da parte della dirigenza, non soltanto il raggiungimento degli obiettivi prefissati, ma anche a suscitare un atteggiamento propositivo per la definizione dei programmi strategici delle singole Amministrazioni. Ogni dirigente di vertice delle strutture in cui si articola

ciascuna amministrazione dovrà essere responsabilizzato per la definizione e per il raggiungimento di precisi obiettivi nei settori indicati dalla presente direttiva, indicando i conseguenti risparmi e le esigenze di formazione del personale. Appare, infatti, indispensabile curare che, attraverso un adeguato programma di formazione tecnica, giuridica e organizzativa, sia assicurato un livello di conoscenza tale da porre la dirigenza in condizione di essere essa stessa motore del cambiamento in atto nell'agire dell'Amministrazione.
Roma, 4 gennaio 2005

Un interessante articolo sul documento informatico.

NUMERO SCHEDA: 5756

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: RIVISTA DI DIRITTO CIVILE

AUTORE: A. Masucci

NUMERO: 5

DATA: 31/10/2004

PAGINA: 749-786

NATURA ATTO: COMMENTO

Si tratta di un articolo interessante e particolareggiato a cura di Alfonso Masucci, intitolato "*Il documento informatico. profili ricostruttivi della nozione e della disciplina*".
Il commento, particolarmente ricco di riferimenti dottrinali e legislativi, affronta, in 19 capitoli, tutti gli aspetti, più o meno controversi, di questo particolare tipo di documento.
Per quanto concerne la parte relativa alle problematiche della sottoscrizione elettronica si segnala il capitolo 14, intitolato "*La particolare disciplina prevista per la sottoscrizione dei documenti delle pubbliche amministrazioni. L'obbligo della firma digitale e i limiti a questo obbligo*".

Pubblicazione sulla Gazzetta Ufficiale del decreto della Presidenza del Consiglio dei Ministri fissante la competenza in materia di certificatori di firma elettronica.

NUMERO SCHEDA: 5267

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: FIRMA DIGITALE

FONTE: GAZZETTA UFFICIALE

NUMERO: 1999

DATA: 25/08/2004

NATURA ATTO: DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

DATA ATTO: 02/07/2004

E' stato pubblicato sulla Gazzetta Ufficiale il decreto del Presidente del Consiglio dei Ministri del 2 Luglio del 2004 che fissa la competenza in materia di certificatori di firma elettronica.
In base ad esso, spetta al Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) la tenuta dell'elenco dei pubblici certificatori di firma elettronica e la cura degli adempimenti relativi all'accreditamento.

Si allega copia del decreto.

PRESIDENZA DEL CONSIGLIO DEI MINISTRI DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE

DECRETO 2 luglio 2004
Competenza in materia di certificatori di firma elettronica.
Art. 1.

1. Il Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) provvede alla tenuta dell'elenco pubblico dei certificatori e cura gli adempimenti connessi, ivi compresi quelli relativi all'accreditamento, previsti dal decreto legislativo 23gennaio 2002, n. 10, dagli articoli 27 e seguenti del decreto del Presidente della Repubblica n. 445 del 2000 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004. 2. Le domande di accreditamento dei certificatori gia' pervenute,ai sensi dell'art. 16 del decreto del Presidente della Repubblica 7aprile 2003, n. 137, al Centro nazionale per l'informatica nella pubblica amministrazione prima del 28 aprile 2004, data di entrata in vigore del decreto del Presidente del Consiglio dei Ministri del 13gennaio 2004, sono istruite e definite dal Centro stesso. Il presente decreto sara' inviato agli organi di controllo per i relativi adempimenti e verra' poi pubblicato nella Gazzetta Ufficiale della Repubblica italiana.
Roma, 2 luglio 2004
Il Ministro: Stanca Registrato alla Corte dei conti il 2 agosto 2004
Ministeri istituzionali - Presidenza del Consiglio dei Ministri,registro n. 8, foglio n. 369

Pubblicato sulla G. U. del 27/04/2004 n. 98 il d.p.c.m. del13/01/2004 concernente "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici".

NUMERO SCHEDA: 4625

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: Firma digitale

FONTE: GAZZETTA UFFICIALE

NUMERO: 98

DATA: 27/04/2004

NATURA ATTO: DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI

DATA ATTO: 27/04/2004

NUM. ATTO: 2004

ORGANO: GOVERNO

SCHEDE COLLEGATE: 3223

Il decreto del presidente del consiglio dei ministri del 13/01/2004, pubblicato sulla Gazzetta Ufficiale del 27/02/2004 n.98, concernente "Regole tecniche per la formazione, trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici" ha reso più sicuro l'utilizzo della firma digitale.
I punti fondamentali del decreto riguardano:

la creazione una coppia di chiavi per la creazione mentre la verifica della firma può essere attribuita ad un solo titolare e la generazione di essa deve essere effettuata con procedure che assicurino unicità e segretezza della chiave privata;

- la verifica delle firme digitali, attraverso il rilascio di una ricevuta che consenta la verifica della firma digitale. Al dipartimento per l'innovazione e le tecnologie della presidenza del consiglio dei ministri una serie di informazioni e documenti tra cui dati anagrafici, ragione sociale, residenza o sede legale e rappresentanza legale, i certificati delle chiavi di certificazione, piano di sicurezza;
- la validazione comporta la generazione di una marca temporale che si applica al risultato della procedura informatica con cui si attribuisce a uno o più documenti informatici, un riferimento temporale opponibile a terzi.

Il testo del d.p.c.m. del 13 gennaio 2004, pubblicato sulla G.U. del 27/04/2004 n. 98 serie generale è consultabile sul sito internet www.gazzettaufficiale.it .

Il TAR Lazio, con sentenza n. 2159 del 08/03/2004, ha stabilito che la disponibilità del bando sul sito internet dell'ente pubblico è sufficiente per l'osservanza del principio della pubblicità adeguata.

NUMERO SCHEDA: 4509

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: TAR LAZIO

DATA: 08/03/2004

RIFERIMENTO NORMATIVO: legge 241/90 e d.lgs. 123/98

NATURA ATTO: SENTENZA

DATA ATTO: 08/03/2004

NUM. ATTO: 2159

ORGANO: TAR LAZIO

La sentenza n. 2159 del TAR Lazio ha affermato che la pubblicazione di un bando sulla gazzetta ufficiale con rinvio alla pubblicazione sul sito internet, non comporta alcuna violazione dell'art. 12 legge 241/90 né dell'art. 5 d.lgs. 123/98, secondo cui la pubblica amministrazione deve predeterminare i requisiti, le modalità e i criteri di attuazione attraverso la pubblicazione in Gazzetta Ufficiale. Pertanto l'avviso che compare sulla gazzetta ufficiale che rinvia al documento integrale consultabile sul sito internet. Il TAR respingendo il ricorso di un consorzio di cooperative onlus contro Sviluppo Italia e il ministero del Lavoro ha stabilito che l'home page dell' ente e la gazzetta ufficiale hanno la stessa dignità.

Si allega il testo della sentenza n. 2159 del 08/03/2004 del TAR Lazio.

F A T T O

Con il presente gravame il Consorzio Fraternità e le Cooperative ricorrenti, impugnano il rigetto della domanda diretta ad ottenere il finanziamento di un progetto; nonché il relativo Bando e le "Modalità di presentazione dei progetti", per l'attuazione del "Progetto Fertilità".

Il ricorso, con tre rubriche di gravame, è affidato alla denuncia della violazione degli artt.2 - 12 della L. n. 241/1990 e dell'art. 5 del d. lgs. n. 123/1998.

La Società Sviluppo Italia S.p.A costituitosi in giudizio il 20 febbraio 2003, in data 24 febbraio 2003 ha versato alcuni atti del provvedimento ed una memoria con cui ha confutato analiticamente i motivi di ricorso.

Il Ministero del lavoro e delle politiche sociali, si è solo formalmente costituito in giudizio.

L'ordinanza della Sezione n. 1057/2003 di rigetto dell'istanza cautelare è stata riformata in appello (ord. n. 3149/2003) della Sesta Sezione che, "sulla scorta di una prima delibazione, attenta in particolare al profilo del periculum", ammetteva con riserva l'istanza del Consorzio alla successiva fase procedimentale.

Con memoria per la discussione del 30 ottobre 2003 Sviluppo Italia ha ribadito la richiesta di rigetto del ricorso.

La parte ricorrente con memoria del 31 Ottobre 2003, ha insistito nelle proprie argomentazioni.

All'udienza del 13 novembre 2003, uditi i patrocinatori delle parti, la causa è stata trattenuta per la decisione.

DIRITTO

Il Consorzio Fraternità Creativa e le Cooperative indicate in epigrafe, in via principale, impugnano il provvedimento ed i relativi atti presupposti, con cui Sviluppo Italia S.pA. ha deliberato la "non accoglibilità" della richiesta di finanziamento del progetto "Un grappolo bresciano" .

In particolare il rigetto dell'istanza è affidato alla duplice considerazione che:

-- non sussistevano "i requisiti di cui all'art. 4, relativamente alla non prevedibilità, se non per un consorzio, di essere tutorato da un altro consorzio" avendo il Consorzio di cooperative sociali previsto di svolgere attività di tutoraggio di una cooperativa sociale;

-- il progetto difettava anche dei requisiti "di cui all'art. 5 del Bando, relativamente alla operatività integrata delle iniziative".

1. Deve preliminarmente d'ufficio rilevarsi, quanto alla giurisdizione, che con sentenza n. 6412 del 25 luglio 2000 (integralmente confermata dal C.d.S. - Sesta Sez. con decisione n. 192 del 22 gennaio 2001), la Sezione ha già ritenuto la propria giurisdizione -- sia pure nei riguardi della Società formalmente dante causa di Sviluppo Italia S.p.A. -- in relazione alla natura di "organismo di diritto pubblico" in senso tecnico.

La Società resistente infatti svolge, sia pure nelle forme di persona giuridica privata, funzioni di sostegno all'economia (selezione e l'incentivazione dell'attività produttiva con contribuzione nazionale e comunitaria) che hanno natura squisitamente pubblicistica a nulla rilevando che la soddisfazione di bisogni generali non esaurisca l'ambito di attività della stessa.

Per tale ragione, anche quando la distribuzione di risorse erariali avvenga con la formula del prestito (modalità del resto utilizzata dal Tesoro fin dagli anni trenta del secolo scorso) tali funzioni non possono essere assolutamente equiparate ad un'attività finanziaria e bancaria (che è invece connotata dall'esclusivo rilievo del conseguimento del profitto) per cui anche l'ottenimento

dell'autorizzazione ad operare ai sensi del testo unico delle leggi in materia bancaria e creditizia emanato con d.lg. 1 settembre 1993 n. 385, è irrilevante ai fini del radicamento della giurisdizione.

2. Nel merito, il ricorso è infondato.

Con il primo motivo di gravame si deducono due differenti profili di ricorso che vanno partitamene confutati.

Viene lamentata innanzitutto la violazione dell'art. 2, II° della L. n. 241/1990 che impone la fissazione del termine di conclusione del procedimento.

La censura è inconferente sul piano della legittimità per provvedimento di non ammissione al contributo. Come la giurisprudenza ha da tempo chiarito, il mancato rispetto del termine previsto dall'art. 2, comma 3, l. 7 agosto 1990 n. 241 per la conclusione dei procedimenti amministrativi determina solo l'illegittimità del silenzio mantenuto dalla p.a. e non anche l'illegittimità del provvedimento tardivamente assunto. E ciò perché il termine per la definizione del procedimento ha carattere meramente acceleratorio, non recando la predetta legge alcuna prescrizione sulla perentorietà del temine, sulla decadenza della potestà amministrativa, o sull'illegittimità del provvedimento adottato (cfr. T.A.R. Lazio, sez. III, 15 gennaio 2003, n. 128; T.A.R. Veneto, sez. I, 20 gennaio 2003, n. 529; T.A.R. Liguria, sez. II, 5 luglio 2002, n. 801, Consiglio Stato, sez. V, 3 giugno 1996, n. 621).

Si sostiene poi l'illegittimità dell'intera procedura, in quanto sulla G.U. parte II° n. 170 del 24 luglio 2001, in luogo del Bando vero e proprio era stato pubblicato un "avviso" il quale rinviava ad un documento "Modalità di presentazione dei progetti" consultabile sul sito internet di Sviluppo Italia.

Tale modalità procedimentale, ad avviso dei ricorrenti, avrebbe violato il combinato disposto dell'art. 12 della L. n. 241/1990 in base al quale l'amministrazione deve predeterminare e pubblicare i criteri per l'erogazione dei contributi; e dell'art. 5 del d.lgs. n. 123/1998 che pone il principio generale dell'ordinamento per cui i requisiti, le modalità e le condizioni concernenti gli interventi attuati con procedimento valutativo debbono esser resi noti con pubblicazione sulla Gazzetta ufficiale. Il rinvio al sito internet non poteva quindi esser legittimamente sostitutivo della sua integrale pubblicazione, non potendo il supporto elettronico garantire i profili di diffusione e di pubblica accessibilità tipici della Gazzetta Ufficiale né tantomeno il carattere dell'ufficialità e della immodificabilità che la pubblicazione conferisce, specialmente con riguardo alle predeterminazione dei criteri di valutazione.

L'assunto non merita adesione.

a) Il principio della "pubblicità adeguata" può dirsi legittimamente assicurato dall'uso del sito internet, dato che il rinvio ad atti, liberamente consultabili sulla rete informatica, di per sé, non costituisce una fattore di diminuzione delle garanzie procedimentali.

L'art. 9 del d.P.R. 28 dicembre 2000 n. 445 concernente il Testo Unico in materia di documentazione amministrativa,infatti, dispone:

-- al primo comma, che gli atti amministrativi informatici "costituiscono informazione primaria ed originale", sancendo così il principio di piena equiparazione sul piano giuridico tra atti amministrativi cartacei e degli atti amministrativi elettronici (la cui accessibilità sulla rete web consente anzi agli interessati sia di conoscere direttamente, ed in tempo reale, tutti i provvedimenti di loro interesse, che di poter gestire i relativi procedimenti);

-- al terzo comma, il principio, di carattere funzionale ed organizzatorio, per cui le pubbliche amministrazioni provvedono a definire, ed a rendere disponibili, per via telematica "moduli e formulari".

Non essendo poi stata allegata dal Consorzio ricorrente alcuna concreta impossibilità, nemmeno temporanea, di loading delle informazioni del bando e delle istruzioni applicative, non ha alcun fondamento giuridico la pretesa mancanza di garanzie di accessibilità al sito internet di Sviluppo Italia non sovvenendo ragioni per ritenere che la gestione di detto sito non abbia rispettato le modalità di cui alla Direttiva del 09/12/2002 sulla "Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali" del Ministero per l'Innovazione Tecnologica.

Neppure le generiche affermazioni circa la mancanza di garanzie dei documenti pubblicati, possono aver rilievo giuridico, non avendo la parte ricorrente al riguardo indicato alcuna modifica in concreto degli atti pubblicati sul sito.

Perde, pertanto consistenza l'obiezione che nell'avviso pubblicato nella Gazzetta Ufficiale fossero assenti i criteri di valutazione dato che tali elementi erano puntualmente contenuti negli atti pubblicati sul sito (cfr. art. 8 del bando di gara, e le pagg. 14 e segg. della Guida esplicativa: all. 3 al deposito Sviluppo Italia del 24 febbraio 2003).

L'onere di pubblicità del procedimento di cui all'art. 12 della L. n. 241/1990 é legittimamente assolto con la pubblicazione sulla G.U. di un avviso diretto a rendere nota l'esistenza di un procedimento

per la concessione di benefici di carattere finanziario, se tale avviso è accompagnato con la messa in libera consultazione sul sito elettronico del bando integrale, delle istruzioni applicative e dei modelli da compilare.

b) Del tutto inconferente è poi, la denunciata violazione dell'art. 5 del Decreto legislativo 31 marzo 1998, n. 123.

In assenza di un diretto e specifico richiamo nel bando, deve escludersi la diretta ed immediata applicabilità alla procedura in questione del d.lgs. n. 123/1998, il quale concerne esclusivamente gli ausili finalizzati al sostegno economico delle "imprese" da parte del Ministero delle Attività Produttive.

Invece il Bando in questione aveva come finalità il sostegno delle attività di inserimento sociale delle persona svantaggiate, da parte del Ministero del Wellfare e non dell'incentivazione delle attività economiche delle imprese,.

Peraltro, si deve rilevare che l'art. 5, erroneamente invocato dalla parte ricorrente, non impone assolutamente l'integrale pubblicazione di tutti gli elementi rilevanti ai fini della selezione nella G.U. ma invece prescrive proprio che "Il soggetto competente comunica i requisiti, le modalità e le condizioni concernenti i procedimenti di cui ai commi 2 e 3, con avviso da pubblicare nella Gazzetta Ufficiale della Repubblica italiana almeno novanta giorni prima dell'invio delle domande, e provvede a quanto disposto dall'art. 2, comma 3".

Il riferimento alla pubblicazione di un "avviso" e non di un "bando" non consente di poter condividere l'assunto di parte ricorrente circa la necessità di una pubblicazione integrale del bando.

Quando il legislatore utilizza il termine "bando" vuole che debbano esser resi noti tutti gli elementi fondamentali del procedimento (e questo il caso ad esempio dell'art. 8 secondo comma d.lgs. n. 157/1995); mentre ricorre alla locuzione "avviso" quando ritiene sufficiente che venga data pubblica notizia del procedimento, rinviando ad altri atti per i dettagli (cfr. ad es. art. 5 primo comma d.lgs. n. 358/1995; art. 8 primo e secondo comma del d.lgs. n. 157 cit.).

L'obbligo procedimentale di pubblicità del procedimento, è esclusivamente limitato alla pubblicazione di una comunicazione (circa l'esistenza e la scadenza del bando per il finanziamento delle iniziative) che assicuri la conoscibilità del procedimento e quindi la par condicio di tutti i soggetti potenzialmente interessati all'inserimento in graduatoria.

In conclusione il motivo è complessivamente infondato e deve essere respinto.

3. Parimenti privo di pregio giuridico appare il secondo motivo con cui il Consorzio ricorrente lamenta che, incongruamente, la S.I. avrebbe ritenuto la pretesa inidoneità di un consorzio a svolgere il tutoraggio di una cooperativa, in quanto:

-) l'art. 4 del Bando, imponeva che il "tutoraggio" di ogni nuova realtà avrebbe dovuto "essere affidata ad un soggetto dotato di adeguata esperienza e di adeguati livelli dimensionali e di efficienza" quale proprio il ricorrente Consorzio;

-) non vi sarebbe alcuna ragione logica dell'affermazione per cui un consorzio (come quello ricorrente, con un'esperienza imprenditoriale più che triennale) non sarebbe stato in grado di esercitare il trasferimento di capacità, esperienza progettuale, e Know-how organizzativo e gestionale nei riguardi di una sola cooperativa.

Irragionevolmente si sarebbe adottato un criterio meramente formale per poter aprioristicamente escludere il progetto "Un Grappolo Bresciano".

L'assunto non ha complessivamente pregio.

In primo luogo l'inequivoca espressione della "lex specialis" del procedimento era tale da ingenerare, nei partecipanti, un assoluto convincimento sulla necessità di redigere le offerte secondo la precisa formulazione dell'art. 4 del bando, che imponeva ad un consorzio di tutelare un altro consorzio e non anche delle cooperative.

La prescrizione era tale da non consentire margini interpretativi nè per Sviluppo Italia che -- una volta posta la norma -- non avrebbe comunque potuto discostarsene; e neppure per gli interessati i quali avrebbero dovuto: o adeguare il progetto alla regola (per esempio indicando, quali tutor delle cooperative sociali, alcune delle imprese costituenti il consorzio delle cooperative sociali); ovvero previamente impugnare una clausola che influiva direttamente sulla ammissibilità stessa del progetto.

Del tutto erroneamente il consorzio -- sulla base di una sua autonoma, soggettiva, valutazione di illogicità della prescrizione -- ha ritenuto di poter del tutto prescindere da una disposizione cogente sulla strutturazione del progetto.

Sul piano della ragionevolezza delle scelte, peraltro, la valutazione circa la maggiore efficacia dell'azione di supporto all'avvio di una cooperativa sociale operata da un tutor costituito in forma di

cooperativa sociale, afferisce a valutazioni di amplia discrezionalità amministrativa, ma non pare violi manifestamente i precetti della logica e della razionalità.
Appare ragionevole che, i consorzi di cooperative sociali facciano da tutor solo ed esclusivamente ad un altro "consorzio di cooperative" (cioè ad un omologa struttura interorganizzativa diretto alla fornitura di servizi consulenziali e di promozione imprenditoriale a favore delle cooperative aderenti); e non possano supportare le "cooperative sociali", che sono tipologie organizzative differenti e distinte (che gestiscono in prima persona servizi socio-sanitari educativi, ed attività finalizzate all'inserimento lavorativo di particolari soggetti "svantaggiati").
Del resto, il fatto che le specifiche criticità organizzative e gestionali che una cooperativa è chiamata ad affrontare siano assolutamente diverse da quelle dei consorzi, è nella specie provato (cfr. pag. 271 e segg. dell'all. 2 al deposito di parte ricorrente del 21 ottobre 2003) dallo stesso Atto costitutivo del Consorzio ricorrente che, tra gli scopi sociali, elenca tutte attività di carattere strumentale e non direttamente operativo (es. stimolare la collaborazione tra le cooperative; realizzare l'inserimento di persone svantaggiate; formazione; commercializzazione dei prodotti, ecc.; informazione sociale; rapporti con il mondo imprenditoriale; promozione di nuove cooperative sociali; fornitura di beni e servizi ai soci; partecipazione agli appalti; ecc.).
Come si vede le attività del Consorzio sono certamente connesse, ma sostanzialmente estranee alla produzione vera e propria dei beni e dei servizi delle cooperative sociali.
In conclusione sul punto, il provvedimento appare del tutto esente dalle dedotte censure di eccesso di potere.
4. Deve infine essere disatteso il terzo motivo di gravame con cui il Consorzio ricorrente lamenta, che Sviluppo Italia avrebbe, erroneamente ed immotivatamente, ritenuto non garantito il rispetto della "operatività integrata delle iniziative".
Al riguardo la giurisprudenza ha costantemente affermato che, in materia di concessione di contributi economici, le valutazioni istruttorie effettuate su base tecnica, comportano scelte tipicamente discrezionali che, come tali, sono sindacabili in sede di legittimità solo per manifesti vizi logici, per errore di fatto, per travisamento dei presupposti, per difetto di istruttoria e, infine, per erronea applicazione delle regole tecniche (Cons. Stato, Sez. VI, 1 marzo 2002, n. 259).
Ciò posto, la motivazione relativa all'assenza di un requisito essenziale espressamente previsto dall'art. 5 u.c., non poteva che essere ricognitiva di tale accertamento negativo.
Al riguardo la parte ricorrente erroneamente assume che l'art. 5 introduceva un criterio che non consentiva a Sviluppo Italia di valutare l'intensità o la qualità dell'integrazione operativa: al contrario Sviluppo Italia doveva puntualmente verificare non solo la completezza della documentazione e dei requisiti per l'ammissione alle agevolazioni ma doveva esercitare una valutazione discrezionale di merito sulla esistenza o meno del requisito della operatività integrata.
In ogni caso la mancata indicazione, da parte dei promotori del progetto, degli elementi dai quali poter ricavare le utilità di scala connessa con l'operatività integrata non può essere supplita con il successivo apodittico, inconferente, e generico richiamo in questa sede al masterplan complessivo del progetto.
Quindi neanche in ricorso, a dimostrazione dell'esattezza dell'assunto, la parte ricorrente ha introdotto riferimenti e particolari, in grado di dimostrare in base a quali elementi concreti potevano ravvisarsi i vantaggi e gli svantaggi derivanti dall'operatività integrata.
Le censure, meramente formali del Consorzio ricorrente sul punto, sono del tutto inconsistenti ad inficiare, sul piano della logica e della razionalità, il provvedimento impugnato.
5. Il ricorso è infondato in tutti i suoi profili e deve in conclusione essere respinto.
In relazione alla novità delle questioni può disporsi l'integrale compensazione delle spese del presente giudizio.

P.Q.M.

il Tribunale Amministrativo Regionale del Lazio – Sez. III^-ter :
1) respinge il ricorso di cui in epigrafe.
2) Spese compensate.
Ordina che la presente sentenza sia eseguita dall'Autorità Amministrativa.
Così deciso dal Tribunale Amministrativo Regionale del Lazio – Sez. III^-ter, in Roma, nella Camera di Consiglio del 13.11.2003.
IL PRESIDENTE dr. Francesco Corsaro
IL CONSIGLIERE-EST. dr. Umberto Realfonzo

Giornale di Diritto Amministrativo - Commento di Angelo Giuseppe Orofino - Firma digitale e rappresentanza in giudizio della P.A.

NUMERO SCHEDA: 4329

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: FIRMA DIGITALE

FONTE: GIORNALE DI DIRITTO AMMINISTRATIVO

AUTORE: Angelo Giuseppe OROFINO

NUMERO: 01/01/2004

DATA: 01/01/2004

PAGINA: 69-73

RIFERIMENTO NORMATIVO: d.P.R. 445/2000

NATURA ATTO: COMMENTO

SCHEDE COLLEGATE: 4285

Gup Tribunale di Firenze – Udienza del 27 maggio 2003. Il Tribunale di Firenze, vista la copia della delibera n. 167 con cui la giunta provinciale voleva costituirsi parte civile, ha stabilito che il documento prodotto dalla giunta provinciale con firma digitale non ha efficacia probatoria circa la provenienza e la volontà dell'Ente, in quanto le disposizioni del d.P.R. 445/2000, disciplinano l'emanazione degli atti con firma digitale la cui esistenza giuridica ha efficacia solo nei rapporti tra la P.A. e i privati con esplicita eccezione, come risulta dalla legge Bassanini 127/1999, dell'autorità giudiziaria.
Il commento di Angelo Giuseppe Orofino, mette in evidenza come nel panorama giurisprudenziale, il numero della pronunce giurisprudenziali in materia di validità informatica dei documenti informatici, sia esiguo. Sicuramente le problematiche procedurali per quello che riguarda i documenti informatici non sono ancora del tutto risolte, ma tutta la normativa finora emanata, a cominciare dal d.P.R. 513/1997 a finire al d.P.R. 445/2000 e successive modifiche, attribuisce pieno valore agli atti amministrativi esternati in forma elettronica, se sottoscritti mediante strumenti idonei ad identificare con sicurezza il sottoscrittore. Probabilmente bisogna cominciare ad intervenire anche sulla cultura dell'utilizzo del documento informatico per consentire a tutti gli operatori del settore della P.A., anche quella giudiziaria, di approcciarsi alla cultura informatica e telematica con una diversa e maggiore consapevolezza.

Pubblicato sulla G.U. il DPR 137/2003 in materia di firma digitale.

NUMERO SCHEDA: 3223

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: Firma digitale

FONTE: ITALIA OGGI

DATA: 18/06/2003

PAGINA: 32

NATURA ATTO: DECRETO PRESIDENTE DELLA REPUBBLICA

DATA ATTO: 07/04/2003

NUM. ATTO: 137

SCHEDE COLLEGATE: 4285; 4625

È stato pubblicato sulla Gazzetta ufficiale n. 138 del 17 giugno 2003 il DPR 7 aprile 2003, n. 137 avente ad oggetto "Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10".
Scopo del provvedimento, che modifica alcuni articoli del Testo unico in materia di documentazione amministrativa, è quello di adeguare il quadro normativo italiano alle disposizioni comunitarie in tema di firma elettronica.
Il provvedimento oltre a liberalizzare l'attività dei soggetti certificatori, non sottoposti a preventiva autorizzazione, disciplina anche il sistema dell'accreditamento al fine del conseguimento di più elevati standard di qualità e sicurezza.
Compiti di vigilanza e di controllo sulla regolare esecuzione delle attività di certificazione e sui certificatori accreditati sono affidati al Dipartimento per l'innovazione e le tecnologie.
Parere favorevole sul regolamento è stato espresso dal Garante per la privacy.

Si veda sul tema la scheda n. 2295.

Approvato dal Consiglio dei Ministri il regolamento di attuazione della direttiva comunitaria n. 93/1999 in materia di firma digitale.

NUMERO SCHEDA: 2295

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: Firma digitale

FONTE: ITALIA OGGI

DATA: 01/02/2003

PAGINA: 5

RIFERIMENTO NORMATIVO: Direttiva CE n. 93/1999

NATURA ATTO: REGOLAMENTO

DATA ATTO: 31/01/2003

ORGANO: CONSIGLIO DEI MINISTRI

Il Consiglio dei Ministri, nella riunione del 31 gennaio 2003, ha approvato il regolamento di attuazione della direttiva comunitaria n. 93/1999, ponendo così le condizioni per l'attivazione concreta dello strumento della firma digitale.
Il regolamento in discorso prevede la liberalizzazione per il settore delle aziende che offrono servizi di certificazione e conferma l'annunciata presenza di due categorie distinte di firma digitale, una "leggera", idonea per l'identificazione personale e l'accesso ai servizi della p.a., l'altra "pesante", necessaria per attribuire il più elevato livello possibile di sicurezza alla sottoscrizione apposta su documenti informatici.
Al riguardo, qui di seguito si riporta un estratto del testo del comunicato ufficiale diramato al termine della riunione del Consiglio dei Ministri:
"...un decreto presidenziale che adegua il quadro normativo italiano delle disposizioni sulla firma elettronica al dettato comunitario, modificando talune parti del testo unico in materia di documentazione amministrativa. Il provvedimento detta una compiuta disciplina in materia di firme elettroniche, di attività dei certificatori (libera e non soggetta ad autorizzazione preventiva) e loro accreditamento, al fine di ottenere il riconoscimento dei requisiti più elevati di qualità e di sicurezza; sarà il Dipartimento per l'innovazione e le tecnologie a vigilare sul corretto svolgimento delle attività di certificazione, ed a controllare periodicamente i certificatori accreditati. Sul provvedimento si è espresso favorevolmente il Consiglio di Stato ed il Garante per la protezione dei dati personali; è stata inoltre esperita, con esito favorevole, la procedura di informazione alla Comunità europea;"

Si allega lo schema di decreto del Presidente della Repubblica.

Schema di decreto del Presidente della Repubblica
concernente regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10
(Approvato dal Consiglio dei ministri il 31.01.2003)

Art. 1

(Modifiche all'articolo 1 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. L'articolo 1 del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, approvato con il decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di seguito denominato: "testo unico", è sostituito dal seguente:

Art. 1 (R)

Definizioni

1. Ai fini del presente testo unico si intende per:
a) DOCUMENTO AMMINISTRATIVO ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa. Le relative modalità di trasmissione sono quelle indicate al capo II, sezione III, del presente testo unico;
b) DOCUMENTO INFORMATICO la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
c) DOCUMENTO DI RICONOSCIMENTO ogni documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare;
d) DOCUMENTO D'IDENTITÀ la carta d'identità ed ogni altro documento munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione competente dello Stato italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale del suo titolare;

e) DOCUMENTO D'IDENTITÀ ELETTRONICO il documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età;
f) CERTIFICATO il documento rilasciato da una amministrazione pubblica avente funzione di ricognizione, riproduzione e partecipazione a terzi di stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche;
g) DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE il documento, sottoscritto dall'interessato, prodotto in sostituzione del certificato di cui alla lettera f) ;
h) DICHIARAZIONE SOSTITUTIVA DI ATTO DI NOTORIETÀ il documento, sottoscritto dall'interessato, concernente stati, qualità personali e fatti, che siano a diretta conoscenza di questi, resa nelle forme previste dal presente testo unico;
i) AUTENTICAZIONE DI SOTTOSCRIZIONE l'attestazione, da parte di un pubblico ufficiale, che la sottoscrizione è stata apposta in sua presenza, previo accertamento dell'identità della persona che sottoscrive;
l) LEGALIZZAZIONE DI FIRMA l'attestazione ufficiale della legale qualità di chi ha apposto la propria firma sopra atti, certificati, copie ed estratti, nonché dell'autenticità della firma stessa;
m) LEGALIZZAZIONE DI FOTOGRAFIA l'attestazione, da parte di una pubblica amministrazione competente, che un'immagine fotografica corrisponde alla persona dell'interessato;
n) FIRMA DIGITALE è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
o) AMMINISTRAZIONI PROCEDENTI le amministrazioni e, nei rapporti con l'utenza, i gestori di pubblici servizi che ricevono le dichiarazioni sostitutive di cui alle lettere g) e h) ovvero provvedono agli accertamenti d'ufficio ai sensi dell'articolo 43;
p) AMMINISTRAZIONI CERTIFICANTI le amministrazioni e i gestori di pubblici servizi che detengono nei propri archivi le informazioni e i dati contenuti nelle dichiarazioni sostitutive, o richiesti direttamente dalle amministrazioni procedenti ai sensi degli articoli 43 e 71;
q) GESTIONE DEI DOCUMENTI l'insieme delle attività finalizzate alla registrazione di protocollo e alla classificazione, organizzazione, assegnazione e reperimento dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato; essa è effettuata mediante sistemi informativi automatizzati;
r) SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti;
s) SEGNATURA DI PROTOCOLLO l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso;
t) CERTIFICATI ELETTRONICI ai sensi dell'articolo 2, comma 1, lettera d) , del decreto legislativo 23 gennaio 2002, n. 10, gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi;
u) CERTIFICATORE ai sensi dell'articolo 2, comma 1, lettera b) , del decreto legislativo 23 gennaio 2002, n. 10, il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;
v) CERTIFICATORE QUALIFICATO il certificatore che rilascia al pubblico certificati elettronici conformi ai requisiti indicati nel presente testo unico e nelle regole tecniche di cui all'articolo 8, comma 2;
z) CERTIFICATORE ACCREDITATO ai sensi dell'articolo 2, comma 1, lettera c) , del decreto legislativo 23 gennaio 2002, n. 10, il certificatore accreditato in Italia ovvero in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE, nonché ai sensi del presente testo unico;
aa) CERTIFICATI QUALIFICATI ai sensi dell'articolo 2, comma 1, lettera e) , del decreto legislativo 23 gennaio 2002, n. 10, i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;
bb) CARTA NAZIONALE DEI SERVIZI il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalla pubblica amministrazione;

cc) FIRMA ELETTRONICA ai sensi dell'articolo 2, comma 1, lettera a) , del decreto legislativo 23 gennaio 2002, n. 10, l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
dd) FIRMA ELETTRONICA AVANZATA ai sensi dell'articolo 2, comma 1, lettera g) , del decreto legislativo 23 gennaio 2002, n. 10, la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;
ee) FIRMA ELETTRONICA QUALIFICATA la firma elettronica avanzata che sia basata su un certificato qualificato e creata mediante un dispositivo sicuro per la creazione della firma;
ff) TITOLARE la persona fisica cui è attribuita la firma elettronica e che ha accesso al dispositivo per la creazione della firma elettronica;
gg) DATI PER LA CREAZIONE DI UNA FIRMA i dati peculiari, come codici o chiavi crittografiche private, utilizzati dal titolare per creare la firma elettronica;
hh) DISPOSITIVO PER LA CREAZIONE DELLA FIRMA il programma informatico adeguatamente configurato (software) o l'apparato strumentale (hardware) usati per la creazione della firma elettronica;
ii) DISPOSITIVO SICURO PER LA CREAZIONE DELLA FIRMA ai sensi dell'articolo 2, comma 1, lettera f) del decreto legislativo 23 gennaio 2002, n. 10, l'apparato strumentale usato per la creazione della firma elettronica, rispondente ai requisiti di cui all'articolo 10 del citato decreto n. 10 del 2002, nonché del presente testo unico;
ll) DATI PER LA VERIFICA DELLA FIRMA i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica;
mm) DISPOSITIVO DI VERIFICA DELLA FIRMA il programma informatico (software) adeguatamente configurato o l'apparato strumentale (hardware) usati per effettuare la verifica della firma elettronica;
nn) ACCREDITAMENTO FACOLTATIVO ai sensi dell'articolo 2, comma 1, lettera h) , del decreto legislativo 23 gennaio 2002, n. 10, il riconoscimento del possesso, da parte del certificatore che lo richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza;
oo) PRODOTTI DI FIRMA ELETTRONICA i programmi informatici (software) , gli apparati strumentali (hardware) e i componenti di tali sistemi informatici, destinati ad essere utilizzati per la creazione e la verifica di firme elettroniche o da un certificatore per altri servizi di firma elettronica.".

Art. 2

(Modifiche all'articolo 8 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. Al comma 2, dell'articolo 8 del testo unico le parole: "sentiti l'Autorità per l'informatica nella pubblica amministrazione", sono sostituite dalle seguenti: ", o, per sua delega del Ministro per l'innovazione e le tecnologie, sentiti il Ministro per la funzione pubblica".

Art. 3

(Modifiche all'articolo 9 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1.Il comma 4 dell'articolo 9 del testo unico è sostituito dal seguente:
"Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite dalla Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, d'intesa con il Dipartimento della funzione pubblica e il Ministero per i beni e le attività culturali, sentito il Garante per la protezione dei dati personali, e, per il materiale classificato, d'intesa con le Amministrazioni della difesa, dell'interno e dell'economia e delle finanze, rispettivamente competenti.".

Art. 4

(Modifiche all'articolo 11 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. Al comma 1 dell'articolo 11 del testo unico le parole "mediante l'uso della firma digitale" sono sostituite dalle seguenti: "mediante l'uso della firma elettronica qualificata".

Art. 5

(Modifiche all'articolo 12 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. L'articolo 12 del testo unico è sostituito dal seguente:
"Art.12 (R) (Pagamenti informatici)
1. Il trasferimento in via telematica di fondi tra privati, pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo regole fissate con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri per la funzione pubblica, della giustizia e dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Banca d'Italia.".

Art. 6

(Modifiche all'articolo 20 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. Al comma 2 dell'articolo 20 del testo unico le parole: "la firma digitale di colui che li spedisce o rilascia, secondo le disposizioni del presente testo unico", sono sostituite dalle seguenti: ", da parte di colui che li spedisce o rilascia, una firma elettronica qualificata.".

Art. 7

(Modifiche alla rubrica della sezione V del capo II del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. La rubrica della sezione V del capo II del testo unico: "Firma digitale" è sostituita dalla seguente: "Firme elettroniche".

Art. 8

(Modifiche all'articolo 22 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. Al comma 1 dell'articolo 22 del testo unico sono apportate le seguenti modificazioni:

a) le lettere b) , c) e d) , sono sostituite dalle seguenti:

"b) per chiavi asimmetriche, la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, utilizzate nell'ambito dei sistemi di validazione di documenti informatici;

c) per chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

d) per chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;";

b) la lettera f) è abrogata;

c) la lettera i) è abrogata;

d) la lettere l) , m) ed n) , sono sostituite dalle seguenti;

"l) per revoca del certificato elettronico, l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi;

m) per sospensione del certificato elettronico, l'operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo;

n) per validità del certificato elettronico, l'efficacia, e l'opponibilità al titolare, dei dati in esso contenuti.";

e) la lettera o) è abrogata.

Art. 9

(Modifiche all'articolo 23 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. L'articolo 23 del testo unico è sostituito dal seguente:

"Articolo 23 (R) (Firma digitale)

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

2. Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica sia stata oggetto dell'emissione di un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

3. L'apposizione ad un documento informatico di una firma elettronica basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

4. L'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.

5. Attraverso il certificato elettronico si devono rilevare, secondo le regole tecniche di cui all'articolo 8, comma 2, la validità del certificato elettronico stesso, nonché gli elementi identificativi del titolare e del certificatore.".

Art. 10

(Modifiche all'articolo 26 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. L'articolo 26 del testo unico è sostituito dal seguente:

"Art. 26 (R) (Certificatori)

1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva, ai sensi dell'articolo 3 del decreto legislativo 23 gennaio 2002, n. 10. Detti certificatori 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 istituti di credito di cui all'articolo 26 del decreto legislativo 1° settembre 1993, n. 385.
2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.
3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente decreto e le relative norme tecniche di cui all'articolo 8, comma 2, e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE.".

Art. 11

(Modifiche all'articolo 27 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. L'articolo 27 del testo unico è sostituito dal seguente:
"Art. 27 (R) (Certificatori qualificati)
1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.
2. I certificatori di cui al comma 1 devono inoltre:
a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;
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 delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate, e che sia in grado di rispettare le norme del presente testo unico e le regole tecniche di cui all'articolo 8, comma 2;
c) applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate;
d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10;
e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi, nei casi in cui il certificatore generi tali chiavi.
3. I certificatori di cui al comma 1 devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al Dipartimento dell'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente testo unico, ai sensi dell'articolo 4, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.
4. Il Dipartimento procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente testo unico e dispone, se del caso, con provvedimento motivato da notificare all'interessato il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.".

Art. 12

(Modifiche al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1.Dopo l'articolo 27 del testo unico è inserito il seguente:
"Art. 27-bis (R) (Certificati qualificati)
1.I certificati qualificati devono contenere almeno le seguenti informazioni:
a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;
b) numero di serie o altro codice identificativo del certificato;
c) nome, ragione o denominazione sociale del certificatore e lo Stato nel quale è stabilito;
d) nome, cognome e codice fiscale del titolare del certificato o uno pseudonimo chiaramente identificato come tale;
e) dati per la verifica della firma corrispondenti ai dati per la creazione della stessa in possesso del titolare;
f) indicazione del termine iniziale e finale del periodo di validità del certificato;
g) firma elettronica avanzata del certificatore che ha rilasciato il certificato.
2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale.

3. Il certificato qualificato può inoltre contenere, su domanda del titolare o del terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:
a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;
b) limiti d'uso del certificato, ai sensi dell'art. 28-bis, comma 3;
c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.".

Art. 13

(Modifiche all'articolo 28 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1.L'articolo 28 del testo unico è sostituito dal seguente:
"Art. 28 (R) (Accreditamento)
1. Ai sensi dell'articolo 5 del decreto legislativo 23 gennaio 2002, n. 10, i certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, possono chiedere di essere accreditati presso la Presidenza del Consiglio dei Ministri-Dipartimento per l'innovazione e le tecnologie, che a tali fini può avvalersi delle strutture pubbliche di cui all'articolo 29.
2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27 ed allegare alla domanda il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole di tecniche.
3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre:
a) avere natura giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, approvato con decreto legislativo 1° settembre 1993, n. 385;
b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti il collegio sindacale, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso istituti di credito ai sensi dell'articolo 26 citato del decreto legislativo 1° settembre 1993, n. 385.
4.La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.
5.Il termine di cui al comma 4 può essere interrotto una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del Dipartimento per l'innovazione e le tecnologie o che questo non possa acquisire autonomamente. In tal caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.
6.A seguito dell'accoglimento della domanda, il Dipartimento per l'innovazione e le tecnologie dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal Dipartimento stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.
7.Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.".

Art. 14

(Modifiche all'articolo 29 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. L'articolo 29 del testo unico è sostituito dal seguente:
"Art. 29 (R) (Vigilanza sull'attività di certificazione)
1. La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, svolge funzioni di vigilanza e controllo sull'attività di certificazione, ai sensi dell'articolo 3, comma 2, del decreto legislativo 23 gennaio 2002, n. 10, anche attraverso le strutture di cui si avvale il Ministro per l'innovazione e le tecnologie.
2.Fatto salvo quanto previsto dal comma 1, il Dipartimento per l'innovazione e le tecnologie provvede al controllo periodico dei certificatori accreditati.".

Art. 15

(Modifiche al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445)

1. Dopo l'articolo 29 del testo unico sono inseriti i seguenti:
"Art. 29-bis (R) (Obblighi del titolare e del certificatore)
1. Il titolare ed il certificatore sono tenuti ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.
2. Il certificatore che rilascia, ai sensi dell'articolo 27, certificati qualificati è tenuto inoltre a:
a) identificare con certezza la persona che fa richiesta della certificazione;

b) rilasciare e rendere pubblico il certificato elettronico nei modi e nei casi stabiliti dalle regole tecniche di cui all'articolo 8, comma 2, nel rispetto della legge 31 dicembre 1996, n. 675 e successive modificazioni;
c) specificare, nel certificato qualificato, su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi;
d) attenersi alle regole tecniche di cui all'articolo 8, comma 2;
e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
f) adottare le misure di sicurezza per il trattamento dei dati personali, ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675;
g) non rendersi depositario di dati per la creazione della firma del titolare;
h) procedere alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni;
i) garantire il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo;
l) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
m) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per dieci anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
n) non copiare, né conservare le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;
o) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore;
p) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.
3. Il certificatore che rilascia certificati al pubblico raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dalla disciplina in materia di dati personali. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.
Art. 29-ter (R) (Uso di pseudonimi)
1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale. Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno dieci anni dopo la scadenza del certificato stesso.
Art. 29-quater (R) (Efficacia dei certificati qualificati)
1. La firma elettronica, basata su un certificato qualificato scaduto, revocato o sospeso non costituisce valida sottoscrizione.
Art. 29-quinquies (R) (Norme particolari per le pubbliche amministrazioni e per
altri soggetti qualificati)
1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:
a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tal fine l'obbligo di accreditarsi ai sensi dell'articolo 28; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione

certificante, al di fuori dei quali sono privi di ogni effetto; con decreto del Presidente del Consiglio dei ministri, su proposta dei Ministri della funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati;
b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.
2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 8, comma 2.
3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei principi generali stabiliti dai rispettivi ordinamenti.
4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche di cui all'articolo 8, comma 2.
Art. 29-sexies (R) Dispositivi sicuri e procedure per la generazione della firma)
1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:
a) sia riservata;
b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;
c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.
2. I dispositivi sicuri di cui al comma 1 devono garantire l'integrità dei dati elettronici a cui la firma si riferisce. I dati devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma.
3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del titolare.
4. I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.
Art. 29-septies (R) (Revoca e sospensione dei certificati qualificati)
1.Il certificato qualificato deve essere a cura del certificatore:
a) revocato in caso di cessazione dell'attività del certificatore;
b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;
c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente decreto;
d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.
2.Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo 8, comma 2.
3.La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.
4.Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all'articolo 8, comma 2.
Art. 29-octies (R) (Cessazione dell'attività)
1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al Dipartimento per l'innovazione e le tecnologie, informando senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.
2. Il certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. L'indicazione di un certificatore sostitutivo non impone la revoca di tutti i certificati non scaduti al momento della cessazione.
3. Il certificatore di cui al comma 1 deve indicare altro depositario del registro dei certificati e della relativa documentazione.
4. Il Dipartimento rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 28, comma 6.".

Art. 16
(Disposizioni transitorie)

1. I certificati emessi alla data di entrata in vigore del presente decreto dai soggetti che risultano iscritti nell'elenco pubblico dei certificatori tenuto dall'Autorità per l'informatica nella pubblica amministrazione sono considerati certificati qualificati.
2. Fino alla completa operatività dell'elenco di cui all'articolo 28, comma 6 del testo unico coloro che intendono accreditarsi presso la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, effettuano gli adempimenti previsti dagli articoli 27 e 28 presso l'Autorità per l'informatica nella pubblica amministrazione.

Art. 17

(Disposizioni finali)

1.Le modifiche di cui al presente regolamento apportate al 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) .

In data 2 agosto 2002 il Consiglio dei Ministri ha approvato uno schema di regolamento per riformare la disciplina della firma digitale.

NUMERO SCHEDA: 1712

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: Firma digitale

FONTE: ITALIA OGGI

NUMERO: 183

DATA: 03/08/2002

PAGINA: 28/31

RIFERIMENTO NORMATIVO: Direttiva CE n. 93/1999; legge n. 50/1999; d.p.r. n. 445/2000; d.lgs. n. 10/2002

NATURA ATTO: SCHEMA DI REGOLAMENTO

DATA ATTO: 02/08/2002

ORGANO: CONSIGLIO DEI MINISTRI

Su proposta del Ministro per l'Innovazione e le Tecnologie, in data 2 agosto 2002, il Consiglio dei Ministri ha concluso l'esame preliminare ed approvato lo schema di Decreto del Presidente della Repubblica intitolato "Regolamento recante modifiche ed integrazioni al testo unico delle disposizioni in materia di documentazione amministrativa, in attuazione del decreto legislativo 23 gennaio 2002, n. 10".
Lo schema di regolamento ridefinisce la disciplina della firma digitale, in recepimento di quanto imposto dalla Direttiva CE n. 93/1999.
Il provvedimento in oggetto -che coordina le disposizioni del D.P.R. n. 445/2000 (Testo Unico in materia di documentazione amministrativa) con quelle del d.lgs. n. 10/2002 sulla firma elettronica- una volta acquisito il parere della Commissione Europea, quello dell'Autorità Garante della privacy, nonché quello del Consiglio di Stato, completerà il suo iter formativo con l'approvazione definitiva da parte del Consiglio dei Ministri e la successiva verifica della Corte dei Conti.
L'entrata in vigore dovrebbe avvenire nel corso del mese di gennaio 2003.

Le principali novità normative previste dallo schema di regolamento in esame sono essenzialmente le seguenti: innanzitutto, si procede a semplificare e liberalizzare il settore dei servizi di certificazione, attraverso l'eliminazione della necessità di un'autorizzazione amministrativa preventiva per l'esercizio dell'attività di certificatore; in secondo luogo, viene prevista la creazione di due distinte tipologie di firma digitale.
Accanto alla tradizionale firma digitale "pesante", procedura più complessa, costosa e sicura (adatta tipicamente ai rapporti P.A./imprese), viene prefigurata l'introduzione di una firma digitale "leggera", idonea ad assicurare l'identificazione personale dei privati e l'accesso di essi ai servizi offerti dalla Pubblica Amministrazione. Tale firma digitale "leggera" si presenta in forma di software contenuto in una smart card, che -per mezzo di un apposito lettore collegato ad un personal computer- consentirà di sottoscrivere qualsiasi tipo di documento elettronico, conferendo al medesimo pieno valore legale.
Piuttosto rilevanti appaiono altresì le innovazioni che saranno verosimilmente introdotte attraverso le disposizioni che dovrebbero costituire il nucleo del futuro articolo 29-quinquies del citato Testo Unico: infatti, secondo il dettato di tali prescrizioni, gli enti pubblici dotati dei necessari mezzi tecnici ed economici potranno richiedere di essere accreditati e -conseguentemente- svolgere direttamente l'attività di certificazione relativa all'uso della firma digitale sui documenti informatici da essi stessi emessi (evitando, in tal modo, di dover ricorrere ad enti di certificazione esterni); inoltre, per quanto concerne la formazione, gestione e sottoscrizione di atti informatici pubblici aventi rilevanza meramente interna alla P.A. emittente, ciascun ente potrà adottare specifiche norme tecniche, nell'esercizio della propria autonomia di organizzazione.
Per consultare il testo:
http://www.filodiritto.com/notizieaggiornamenti/agosto2002/schemadprmodificafirmadigitale.htm

Firma on-line, due pesi e due misure.

NUMERO SCHEDA: 1172

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: FIRMA DIGITALE

FONTE: ITALIA OGGI

NUMERO: 52

DATA: 02/03/2002

PAGINA: 35

RIFERIMENTO NORMATIVO: d.p.r. 445/2000; art. 2702 codice civile

NATURA ATTO: DECRETO LEGISLATIVO

DATA ATTO: 23/01/2002

NUM. ATTO: 10

Il d.lgs. 10/2002, entrato in vigore il 02/03/2002, recependo la direttiva comunitaria 1999/93/CE, apporta due novità di rilievo alla normativa nazionale del settore atteso che da un lato, disciplina sia la firma digitale"pesante" che quella cosiddetta "leggera", dall'altro modifica il d.p.r.445/2000, proprio sulla base dell'utilizzo della firma elettronica.
L'art. 2 lettera a) del decreto legislativo in esame definisce la firma elettronica "leggera " come: "l'insieme dei dati in forma elettronica allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica".
Il medesimo articolo alla lettera g) definisce la firma elettronica avanzata o "pesante" come quella "ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione (…)".
L'allegazione della firma digitale "pesante" o "leggera" comporta rilevanti differenze sul valore probatorio del documento elettronico sottoscritto : infatti l'art. 6, che modifica l'art. 10 del d.p.r. 445/2000, stabilisce che il documento informatico soddisfa il requisito della forma scritta solo se sottoscritto con firma elettronica.
Sempre il comma 2 del testo novellato dell'art. 10 del d.p.r. 445/2000, disciplina il valore probatorio del documento a cui è apposta la firma digitale leggera: detto documento è liberamente valutabile, considerate le caratteristiche oggettive di qualità e sicurezza. Pertanto il documento non fornirà piena prova ma costituirà soltanto un elemento probatorio.
Al contrario i documenti sottoscritti con firma digitale "pesante" faranno piena prova della provenienza delle dichiarazioni in essi contenute, fino a querela di falso. La disciplina equipara i documenti sottoscritti in questo modo alle scritture private autenticate di cui all'art. 2702 codice civile, ma attribuisce loro un valore probatorio ancora più ampio.
Infatti, il documento sottoscritto con la firma digitale avanzata non è soggetto alla condizione che il soggetto contro il quale è prodotto riconosca la sottoscrizione, né che occorra un riconoscimento legale alla stessa. D'altra parte lo scopo della firma digitale è proprio quello di sostituire con le procedure informatiche i mezzi ordinari utilizzati per il riconoscimento ed il disconoscimento delle firme autografe su cartaceo.
Il decreto legislativo completa la riforma novellando il testo dell'art. 38 del d.p.r. 445/2000 , il quale, nella nuova formulazione, stabilisce che le dichiarazioni inviate per via telematica sono valide solo se sottoscritte con la firma digitale "pesante".
Al contrario, le dichiarazioni sostitutive convalidate con la firma "leggera" saranno utilizzabili ai fini istruttori ma non potranno costituire una valida istanza volta ad ottenere i benefici di cui alle dichiarazioni sostitutive regolarmente formate.

Il testo del decreto del Presidente della Repubblica 7 aprile 2003, n.137 "Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10", (Pubblicato sulla Gazzetta Ufficiale del 17 giugno 2003, n.138) è allegato alla scheda n. 2295).

La firma digitale ed il testo unico sulla documentazione amministrativa

NUMERO SCHEDA: 140

CLASSIFICAZIONE: E – GOVERNMENT

SOTTOCLASSIFICAZIONE: FIRMA DIGITALE

FONTE: CONSIGLIO DEI MINISTRI

RIFERIMENTO NORMATIVO: DPR 513/97; L.15/68

NATURA ATTO: TESTO UNICO

DATA ATTO: 25/08/2000

SCHEDE COLLEGATE: 6085

Il D.P.R 445/2000 raccoglie le disposizioni legislative e regolamentari contenute rispettivamente nel d.lgs. 443/2000 e nel D.P.R. 444/2000. Il Capo II, sezione V, qui di seguito riportata nella versione aggiornata con le modifiche apportate dal d.p.r. 137/2003, contiene la disciplina generale della firma digitale, comprese le disposizioni sulla sicurezza e sulla responsabilità dei certificatori.

Capo II Sez. V FIRMA DIGITALE	Capo II Sez. V FIRME ELETTRONICHE
Articolo 22 (R) – Definizioni	
1. Ai fini del presente Testo unico si intende: a) per sistema di validazione, il sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità;	1. Ai fini del presente Testo unico si intende: a) per sistema di validazione, il sistema informatico e crittografico in grado di generare e apporre la firma digitale o di verificarne la validità;
b) per chiavi asimmetriche, la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici;	b) per chiavi asimmetriche, la coppia di chiavi crittografiche, una privata e una pubblica, correlate tra loro, utilizzate nell'ambito dei sistemi di validazione di documenti informatici;
c) per chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica.	c) per chiave privata, l'elemento della coppia di chiavi asimmetriche, destinato a essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;
d) per chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi;	d) per chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato a essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;
f) per certificazione, il risultato della procedura informatica, applicata alla chiave	ABROGATA

procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni;	
g) per validazione temporale, il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi;	f) per validazione temporale, il risultato della procedura informatica, con cui si attribuiscono, a uno o più documenti informatici, una data e un orario opponibili ai terzi;
h) per indirizzo elettronico, l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici;	g) per indirizzo elettronico, l'identificatore di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici;
i) per certificatore, il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati;	ABROGATA
l) per revoca del certificato, l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi;	l) per revoca del certificato elettronico, l'operazione con cui il certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi;
m) per regole tecniche, le specifiche di carattere tecnico, ivi compresa ogni disposizione che ad esse si applichi.	m) per sospensione del certificato elettronico, l'operazione con cui il certificatore sospende la validità del certificato per un determinato periodo di tempo;
n) per validità del certificato, l'efficacia, e l'opponibilità al titolare della chiave pubblica, dei dati in esso contenuti;	n) per validità del certificato elettronico, l'efficacia e l'opponibilità al titolare dei dati in esso contenuti.
o) per regole tecniche, le specifiche di carattere tecnico, ivi compresa ogni disposizione che ad esse si applichi.	ABROGATA
Articolo 23 (R) - Firma digitale	
1. A ciascun documento informatico, o a un gruppo di documenti informatici, nonché al duplicato o copia di essi, può essere apposta, o associata con separata evidenza informatica, una firma digitale.	1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo.	2. Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica sia stata oggetto dell'emissione di un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.
3. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.	3. L'apposizione ad un documento informatico di una firma elettronica basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante o chi richiede la

	pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.
4. Per la generazione della firma digitale deve adoperarsi una chiave privata la cui corrispondente chiave pubblica non risulti scaduta di validità ovvero non risulti revocata o sospesa ad opera del soggetto pubblico o privato che l'ha certificata.	4. L'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.
5. L'uso della firma apposta o associata mediante una chiave revocata, scaduta o sospesa equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.	5. Attraverso il certificato elettronico si devono rilevare, secondo le regole tecniche di cui all'articolo 8, comma 2, la validità del certificato elettronico stesso, nonché gli elementi identificativi del titolare e del certificatore.
6. L'apposizione di firma digitale integra e sostituisce, ad ogni fine previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere.	ELIMINATO
7. Attraverso la firma digitale devono potersi rilevare gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione.	ELIMINATO
Articolo 26 (R) - Deposito della chiave privata	Art. 26 (R) – Certificatori
1. Il titolare della coppia di chiavi asimmetriche può ottenere il deposito in forma segreta della chiave privata presso un notaio o altro pubblico depositario autorizzato.	1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva, ai sensi dell'articolo 3 del decreto legislativo 23 gennaio 2002, n. 10. Detti certificatori 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, approvato con decreto legislativo 1° settembre 1993, n. 385.
2. La chiave privata di cui si richiede il deposito può essere registrata su qualsiasi tipo di supporto idoneo a cura del depositante e deve essere consegnata racchiusa in un involucro sigillato in modo che le informazioni non possano essere lette, conosciute od estratte senza rotture od alterazioni.	2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.
3. Le modalità del deposito sono regolate dalle disposizioni dell'articolo 605 del codice civile, in quanto applicabili.	3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente decreto e le relative norme tecniche di cui all'articolo 8, comma 2, e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE.

Articolo 27 (R) - Certificazione delle chiavi	Art. 27 (R) - Certificatori qualificati
1. Chiunque intenda utilizzare un sistema di chiavi asimmetriche di cifratura con gli effetti di cui all'articolo 8, comma 1 deve munirsi di una idonea coppia di chiavi e rendere pubblica una di esse mediante la procedura di certificazione.	1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.
2. Le chiavi pubbliche di cifratura sono custodite per un periodo non inferiore a dieci anni a cura del certificatore e, dal momento iniziale della loro valultabili in forma telematica.	2. I certificatori di cui al comma 1 devono inoltre: a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione; 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 delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate, e che sia in grado di rispettare le norme del presente testo unico e le regole tecniche di cui all'articolo 8, comma 2; c) applicare procedure e metodi amministrativi e di gestione adeguati e tecniche consolidate; d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10; e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi, nei casi in cui il certificatore generi tali chiavi.
3. Salvo quanto previsto dall'articolo 29, le attività di certificazione sono effettuate da certificatori inclusi, sulla base di una dichiarazione anteriore all'inizio dell'attività, in apposito elenco pubblico, consultabile in via telematica, predisposto tenuto e aggiornato a cura dell'Autorità per l'informatica nella pubblica amministrazione, e dotati dei seguenti requisiti, specificati con il decreto di cui all'articolo 8: a) forma di società per azioni e capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione all'attività bancaria, se soggetti privati; b) possesso da parte dei rappresentanti legali e dei soggetti preposti all'amministrazione, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche; c) affidamento che, per competenza ed esperienza, i responsabili tecnici del certificatore e il personale addetto all'attività di certificazione siano in grado di rispettare le norme del presente regolamento e le regole	3. I certificatori di cui al comma 1 devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al Dipartimento dell'innovazione e le tecnologie della Presidenza del Consiglio dei Ministri, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente testo unico, ai sensi dell'articolo 4, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.

norme del presente regolamento e le regole tecniche di cui all'articolo 8; d) qualità dei processi informatici e dei relativi prodotti, sulla base di standard riconosciuti a livello internazionale.	
4. La procedura di certificazione di cui al comma 1 può essere svolta anche da un certificatore operante sulla base di licenza o autorizzazione rilasciata da altro Stato membro dell'Unione europea o dello Spazio economico europeo, sulla base di equivalenti requisiti.	4. Il Dipartimento procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente testo unico e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.
	Art. 27-bis (R) - Certificati qualificati
	1. I certificati qualificati devono contenere almeno le seguenti informazioni: a) indicazione che il certificato elettronico rilasciato è un certificato qualificato; b) numero di serie o altro codice identificativo del certificato; c) nome, ragione o denominazione sociale del certificatore e lo Stato nel quale è stabilito; d) nome, cognome e codice fiscale del titolare del certificato o uno pseudonimo chiaramente identificato come tale; e) dati per la verifica della firma corrispondenti ai dati per la creazione della stessa in possesso del titolare; f) indicazione del termine iniziale e finale del periodo di validità del certificato; g) firma elettronica avanzata del certificatore che ha rilasciato il certificato.
	2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale.
	3. Il certificato qualificato può inoltre contenere, su domanda del titolare o del terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto: a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza; b) limiti d'uso del certificato, ai sensi dell'articolo 28-bis, comma 3; c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

Articolo 28 (R) - Obblighi dell'utente e del certificatore	Art. 28 (R) - Accreditamento
1. Chiunque intenda utilizzare un sistema di chiavi asimmetriche o della firma digitale, è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.	1. Ai sensi dell'articolo 5 del decreto legislativo 23 gennaio 2002, n. 10, i certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, possono chiedere di essere accreditati presso la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, che a tali fini può avvalersi delle strutture pubbliche di cui all'articolo 29.
2. Il certificatore è tenuto a: a) identificare con certezza la persona che fa richiesta della certificazione; b) rilasciare e rendere pubblico il certificato avente le caratteristiche fissate con il decreto di cui all'articolo 8; c) specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite; d) attenersi alle regole tecniche di cui all'articolo 8; e) informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi; f) attenersi alle misure minime di sicurezza per il trattamento dei dati personali,emanate ai sensi dell'articolo 12, comma 2 della legge 31 dicembre 1996, n. 675; g) non rendersi depositario di chiavi private; h) procedere tempestivamente alla revoca od alla sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni; i) dare immediata pubblicazione della revoca e della sospensione della coppia di chiavi asimmetriche; l) dare immediata comunicazione all'Autorità per l'informatica nella pubblica amministrazione ed agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività e della conseguente rilevazione della documentazione da parte di altro certificatore o del suo annullamento.	2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27 ed allegare alla domanda il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole di tecniche.
	3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre: a) avere natura giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, approvato con decreto legislativo

	bancaria e creditizia, approvato con decreto legislativo 1° settembre 1993, n. 385; b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti il collegio sindacale, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 citato del decreto legislativo 1° settembre 1993, n. 385.
	4. La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.
	5. Il termine di cui al comma 4 può essere interrotto una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del Dipartimento per l'innovazione e le tecnologie o che questo non possa acquisire autonomamente. In tal caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.
	6. A seguito dell'accoglimento della domanda, il Dipartimento per l'innovazione e le tecnologie dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal Dipartimento stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.
	7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.
	Art. 28-bis (L) Responsabilità del certificatore
	1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa, del danno cagionato a chi abbia fatto ragionevole affidamento: a) sull'esattezza delle informazioni in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati; b) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato; c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi.
	2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano ragionevole affidamento sul certificato stesso, dei danni provocati per effetto della mancata registrazione della revoca e sospensione del certificato

	registrazione della revoca o sospensione del certificato, salvo che provi d'aver agito senza colpa.
	3. Il certificatore può indicare, in un certificato qualificato, i limiti d'uso di detto certificato ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.
Articolo 29 (R) - Chiavi di cifratura della pubblica amministrazione	Art. 29 (R) - Vigilanza sull'attività di certificazione
1. Le pubbliche amministrazioni provvedono autonomamente, con riferimento al proprio ordinamento, alla generazione, alla conservazione, alla certificazione ed all'utilizzo delle chiavi pubbliche di competenza.	1. La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, svolge funzioni di vigilanza e controllo sull'attività di certificazione, ai sensi dell'articolo 3, comma 2, del decreto legislativo 23 gennaio 2002, n. 10, anche attraverso le strutture di cui si avvale il Ministro per l'innovazione e le tecnologie.
2. Con il decreto di cui all'articolo 8 sono disciplinate le modalità di formazione, di pubblicità, di conservazione, certificazione e di utilizzo delle chiavi pubbliche delle pubbliche amministrazioni.	2. Fatto salvo quanto previsto dal comma 1, il Dipartimento per l'innovazione e le tecnologie provvede al controllo periodico dei certificatori accreditati.
3. Le chiavi pubbliche dei pubblici ufficiali non appartenenti alla pubblica amministrazione sono certificate e pubblicate autonomamente in conformità alle leggi ed ai regolamenti che definiscono l'uso delle firme autografe nell'ambito dei rispettivi ordinamenti giuridici.	ELIMINATO
4. Le chiavi pubbliche di ordini ed albi professionali legalmente riconosciuti e dei loro legali rappresentanti sono certificate e pubblicate a cura del Ministro di grazia e giustizia o suoi delegati.	ELIMINATO
	Art. 29-bis (R) - Obblighi del titolare e del certificatore
	1. Il titolare e il certificatore sono tenuti ad adottare tutte le misure organizzative e tecniche idonee a evitare danno ad altri.
	2. Il certificatore che rilascia, ai sensi dell'articolo 27, certificati qualificati è tenuto inoltre a: a) identificare con certezza la persona che fa richiesta della certificazione; b) rilasciare e rendere pubblico il certificato elettronico nei modi e nei casi stabiliti dalle regole tecniche di cui all'articolo 8, comma 2, nel rispetto della legge 31 dicembre 1996, n. 675, e successive modificazioni; c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi; d) attenersi alle regole tecniche di cui all'articolo 8

	d) attenersi alle regole tecniche di cui all'articolo 8, comma 2; e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione; f) adottare le misure di sicurezza per il trattamento dei dati personali, ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675; g) non rendersi depositario di dati per la creazione della firma del titolare; h) procedere alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni; i) garantire il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo; l) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici; m) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per dieci anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari; n) non copiare, nè conservare le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione; o) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore; p) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato

	3. Il certificatore che rilascia certificati al pubblico raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dalla disciplina in materia di dati personali. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.
	Art. 29-ter (R) - Uso di pseudonimi
	1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale. Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno dieci anni dopo la scadenza del certificato stesso.
	Art. 29-quater (R) - Efficacia dei certificati qualificati
	1. La firma elettronica, basata su un certificato qualificato scaduto, revocato o sospeso non costituisce valida sottoscrizione.
	Art. 29-quinquies (R) - Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati
	1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni: a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell'articolo 28; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati; b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.
	2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 8, comma 2.
	3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e

	per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei principi generali stabiliti dai rispettivi ordinamenti.
	4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche di cui all'articolo 8, comma 2.
	Art. 29-sexies (R) - Dispositivi sicuri e procedure per la generazione della firma
	1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata: a) sia riservata; b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni; c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.
	2. I dispositivi sicuri di cui al comma 1 devono garantire l'integrità dei dati elettronici a cui la firma si riferisce. I dati devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma.
	3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del titolare.
	4. I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione di cui all'articolo 10, comma 1, del decreto legislativo 23 gennaio 2002, n. 10.
	Art. 29-septies (R) - Revoca e sospensione dei certificati qualificati
	1. Il certificato qualificato deve essere a cura del certificatore: a) revocato in caso di cessazione dell'attività del certificatore; b) revocato o sospeso in esecuzione di un provvedimento dell'autorità; c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente decreto; d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni;
	2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo 8, comma 2.
	3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.

	adeguato riferimento temporale.
	4. Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all'articolo 8, comma 2.
	Art. 29-octies (R) - Cessazione dell'attività
	1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al Dipartimento per l'innovazione e le tecnologie, informando senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.
	2. Il certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. l'indicazione di un certificatore sostitutivo non impone la revoca di tutti i certificati non scaduti al momento della cessazione.
	3. Il certificatore di cui al comma 1 deve indicare altro depositario del registro dei certificati e della relativa documentazione.
	4. Il dipartimento rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 28, comma 6.
Articolo 36 (L) Carta d'identità e documenti elettronici	
1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica e del documento d'identità elettronico sono definite con decreto del Presidente del Consiglio dei Ministri su proposta del Ministro dell'interno, di concerto con il Ministro della funzione pubblica, sentito il Garante per la protezione dei dati personali.	1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica, del documento d'identità elettronico e della carta nazionale dei servizi sono definite con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, con il Ministro per l'innovazione e le tecnologie e con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali
e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti ivi compresa la chiave biometrica, occorrenti per la firma digitale;	e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica.
4. La carta d'identità elettronica può altresì essere utilizzata per il trasferimento elettronico dei pagamenti tra soggetti privati e pubbliche amministrazioni.	4. La carta d'identità elettronica e la carta nazionale dei servizi possono essere utilizzate ai fini dei pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalità stabilite con decreto del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.
5. Con decreto del Ministro dell'interno, sentiti l'Autorità per l'informatica nella pubblica amministrazione, il Garante per la protezione dei dati personali e la Conferenza Stato-città ed autonomie locali, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la	5. Con decreto del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Conferenza Stato-città ed autonomie locali, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta di identità elettronica, del

tecnologie e ai materiali utilizzati per la produzione delle carte di identità e dei documenti di riconoscimento di cui al presente articolo. Le predette regole sono adeguate con cadenza almeno biennale in relazione alle esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche.	per la produzione della carta di identità elettronica, del documento di identità elettronico e della carta nazionale dei servizi.
Articolo 38 (L-R) - Modalità di invio e sottoscrizione delle istanze	
2. Le istanze e le dichiarazioni inviate per via telematica sono valide se sottoscritte mediante la firma digitale o quando il sottoscrittore è identificato dal sistema informatico con l'uso della carta d'identità elettronica.	2. Le istanze e le dichiarazioni inviate per via telematica sono valide: a) se sottoscritte mediante la firma digitale, basata su di un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura; b) ovvero quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi (L).

CAPITOLO IV

POSTA ELETTRONICA

L'e-mail è ormai lo strumento di comunicazione elettronica più utilizzato per lo scambio di comunicazioni[1].

La posta elettronica o e-mail (acronimo di Electronic Mail) è un mezzo di comunicazione in forma scritta via Internet, che ha come principale vantaggio quello dell'immediatezza.

I messaggi possono includere testo, immagini, audio, video o qualsiasi tipo di file.

La Posta Elettronica Certificata (PEC) è un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici. "Certificare" l'invio e ricezione - i due momenti fondamentali nella trasmissione dei documenti informatici - significa fornire al mittente, dal proprio gestore di posta, una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione.

Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna con precisa indicazione temporale. Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte venga conservata per un periodo di tempo definito a cura dei gestori, con lo stesso valore giuridico delle ricevute.

La fase di sperimentazione.

Avviata nel 2002 dal Centro Tecnico per la Rupa (Rete Unitaria per la Pubblica Amministrazione) attraverso l'attività pluriennale del Gruppo di Lavoro ivi costituito, la prima sperimentazione sul servizio di PEC è stata condotta con particolare riguardo agli aspetti legati all' interoperabilità ed ha prodotto una serie di documenti tecnici. Parallelamente sono stati sviluppati, nell'ambito della PA, alcuni progetti che hanno realizzato servizi di posta elettronica certificata partendo dalle regole tecniche che si

[1] L'introduzione al capitolo relativo alla posta elettronica è tratta dalla sezione dedicata all'argomento del sito del CNIPA, il Centro Nazionale per l'Informatica nella Pubblica Amministrazione. La scelta è dovuta alla chiarezza espositiva con la quale viene introdotto un argomento che presenta problematiche tecniche di non immediata comprensione.

andavano formando. Le attività sperimentali hanno coinvolto numerosi fornitori di soluzioni. Un tale approccio, decisamente innovativo per il panorama italiano, ha consentito di mettere a punto una norma essendo da un lato coscienti della reale applicabilità (e nel contempo avendo già fatto maturare da un lato le possibilità di impiego della tecnologia) e dall'altro la crescita di un mercato.

La normativa di riferimento.

Su proposta del Ministro per l'Innovazione e le Tecnologie di concerto con il Ministro per la Funzione Pubblica, il Consiglio dei Ministri nella seduta del 28 gennaio 2005 ha approvato in via definitiva un provvedimento che intende disciplinare le modalità di utilizzo della Posta Elettronica Certificata (PEC) non solo nei rapporti con la PA, ma anche tra privati cittadini. In sintesi le novità contenute nel DPR dell'11 febbraio 2005, n. 68 pubblicato su G.U. del 28 aprile 2005, n. 97:

- *nella catena di trasmissione potranno scambiarsi le e-mail certificate sia i privati, sia le PA. Saranno i gestori del servizio (art. 14), iscritti in apposito elenco tenuto dal CNIPA (che verificherà i requisiti soggettivi ed oggettivi inerenti ad esempio alla capacità ed esperienza tecnico-organizzativa, alla dimestichezza con procedure e metodi per la gestione della sicurezza, alla certificazione ISO9000 del processo), a fare da garanti dell'avvenuta consegna. Per iscriversi all'elenco dovranno possedere un capitale sociale minimo non inferiore a un milione di euro e presentare una polizza assicurativa contro i rischi derivanti dall'attività di gestore;*
- *i messaggi verranno sottoscritti con la firma digitale avanzata che dovrà essere apposta sia sulla busta, sia sulle ricevute rilasciate dai gestori per assicurare l'integrità e l'autenticità del messaggio;*
- *i tempi di conservazione: i gestori dovranno conservare traccia delle operazioni per 30 mesi;*
- *i virus: i gestori sono tenuti a verificare l'eventuale presenza di virus nelle e-mail ed informare in caso positivo il mittente, bloccandone la trasmissione (art. 12);*
- *le imprese, nei rapporti intercorrenti, potranno dichiarare l'esplicita volontà di accettare l'invio di PEC mediante indicazione nell'atto di iscrizione delle imprese.*

Le regole tecniche.

Le nuove regole tecniche saranno oggetto di un DPCM e conterranno tutti i requisiti tecnico-funzionali che devono essere rispettati dalle piattaforme utilizzate per erogare il servizio. Il Cnipa ha predisposto la proposta di schema di decreto sulle Regole tecniche, approvato dal Collegio il 12 maggio 2005. L'atto è in via di notifica ai competenti uffici della Commissione Europea così come previsto dall'iter legislativo che prevede ancora vari passi. Al termine di questo processo e con la pubblicazione in G.U. del decreto si aprirà la possibilità, per gli operatori di mercato in possesso dei requisiti previsti dalla legge, di qualificarsi quali gestori di PEC.

Il CNIPA effettuerà le attività di vigilanza e controllo assegnategli dalla norma e, con un apposito Centro di competenza, supporterà le PA ai fini dell'introduzione della PEC nei procedimenti amministrativi.

Anche il Codice dell'Amministrazione Digitale contiene disposizioni in materia di posta elettronica certificata: si segnalano, in particolare, l'art. 6 (Utilizzo della posta elettronica certificata) e 48 (posta elettronica certificata).

Il Codice dell'Amministrazione digitale contiene disposizioni in materia di posta elettronica certificata.

NUMERO SCHEDA: 6570

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: POSTA ELETTRONICA

NATURA ATTO: DECRETO LEGISLATIVO

DATA ATTO: 07/03/2005

NUM. ATTO: 82

Il Codice dell'amministrazione digitale (d.lgs. n. 82/2005), che entrerà in vigore il primo gennaio 2006, contiene importanti disposizioni in materia di posta elettronica certificata.

Si segnalano, in particolare, l'art. 6 (Utilizzo della posta elettronica certificata) e 48 (Posta elettronica certificata), dei quali si allega il testo.

6. *Utilizzo della posta elettronica certificata.*
1. Le pubbliche amministrazioni centrali utilizzano la posta elettronica certificata, di cui al *decreto del Presidente della Repubblica 11 febbraio 2005, n. 68*, per ogni scambio di documenti e informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata.
2. Le disposizioni di cui al comma 1 si applicano anche alle pubbliche amministrazioni regionali e locali salvo che non sia diversamente stabilito.
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*.
2. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata 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.

Il Governo ha approvato il regolamento che attribuisce all'invio on line di documenti lo stesso valore di una notificazione a mezzo posta.

NUMERO SCHEDA: 5859

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: INFORMATIZZAZIONE P.A.

FONTE: CONSIGLIO DEI MINISTRI

DATA: 28/01/2005

NATURA ATTO: DECRETO PRESIDENTE DELLA REPUBBLICA

Il Decreto del Presidente della Repubblica, approvato dal governo in data 28 Gennaio 2005, attribuisce pieno valore legale alla posta elettronica certificata, nei rapporti fra cirttadini e p.a., fra uffici pubblici e fra privati.
La trasmissione telematica avrà il medesimo valore di una notificazione a mezzo posta: in particolare le ricevute di posta elettronica saranno sottoscritte dai gestori mediante firma digitale.
Il servizio potrà essere offerto soltanto dai gestori della posta elettronica certificata cioè da soggetti pubblici o privati iscritti ad apposito elenco tenuto dal Cnipa (Centro nazionale per l'informatica nella p.a.). Detti gestori dovranno conservare per 30 mesi la traccia delle operazioni informatiche in un apposito registro.
Si segnala che sul sito del Governo è reperibile un dossier intitolato "Dossier su posta_elettronica e_p.a." , consultabile al seguente indirizzo:
http://www.governo.it/GovernoInforma/Dossier/posta_elettronica_pa/index.html

Si allega il testo integrale del regolamento.

D.P.R. 11 febbraio 2005, n. 68

Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della *L. 16 gennaio 2003, n. 3.*

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 è 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, nonché 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.
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.
3. *Trasmissione del documento informatico.*
1. Il comma 1 dell'articolo 14 del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*, è 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.».
4. *Utilizzo della posta elettronica certificata.*
1. La posta elettronica certificata consente l'invio di messaggi la cui trasmissione è 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, è 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 è 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.
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.
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 è 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 è 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 è 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'articolo 14, comma 2, del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*.

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.

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.

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 è 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.

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.

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.

12. *Virus informatici.*

1. Qualora il gestore del mittente riceva messaggi con virus informatici è 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 è tenuto a non inoltrarli al destinatario, informando tempestivamente il gestore del mittente, affinché 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.

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.

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 àmbito 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 è comunicata al CNIPA entro il quindicesimo giorno.
12. Il venire meno di uno o più requisiti tra quelli indicati al presente articolo è 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.
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. È 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.

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.

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 è acquisito il concerto del Ministro delle comunicazioni.

18. Disposizioni finali.

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 Consiglio dei Ministri ha approvato in data 25/03/2004 lo schema di decreto sulla validità legale della posta elettronica.

NUMERO SCHEDA: 4524

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: POSTA ELETTRONICA

FONTE: ITALIA OGGI

AUTORE: Andrea MASCOLINI

DATA: 26/03/2004

PAGINA: 25

NATURA ATTO: COMMENTO

Il Consiglio dei ministri ha approvato lo schema di decreto di introduzione della posta elettronica come documentazione legalmente valida nei rapporti della P.A. e tra i cittadini e la stessa P.A.

I punti fondamentali del decreto sono i seguenti :

- possibilità, tramite la posta elettronica certificata, di inviare messaggi la cui trasmissione è valida agli effetti di legge;

- possibilità di usufruire di tale risorsa anche ai cittadini nei rapporti con la P.A.;
- istituzione dell'elenco dei gestori di posta elettronica certificata presso il Comitato nazionale per l'informatica nella P.A. (Cnipa);
- accesso all'elenco previa richiesta e prova di appositi requisiti tecnici di affidabilità e forma giuridica di società di capitali. L'accesso viene concesso con il silenzio assenso entro 30 giorni dall'invio della domanda;
- validità giuridica delle ricevute di consegna e spedizione rilasciate dai gestori;
- esclusione dell'applicazione del regolamento per i processi civili, amministrativi e davanti alla Corte dei Conti;
- la trasmissione e la ricezione del messaggio di posta elettronica si intende certificata se attestata dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna rilasciata da un gestore autorizzato;
- in caso di smarrimento della ricevuta la traccia informatica sarà custodita per 24 mesi in un apposito registro informatico custodito dai gestori, con lo stesso valore giuridico delle ricevute.

L'e-mail può costituire una promessa unilaterale di pagamento? (decreto ingiuntivo del Tribunale di Cuneo).

NUMERO SCHEDA: 4285

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE:

FONTE: ALTALEX

NUMERO: 563

DATA: 28/01/2004

RIFERIMENTO NORMATIVO: d.p.r. 445/2000

NATURA ATTO: DECRETO

DATA ATTO: 15/12/2003

ORGANO: TRIBUNALE

SCHEDE COLLEGATE: 3223; 4192; 4329; 6162

Il Tribunale di Cuneo, con decreto ingiuntivo del 15 dicembre 2003, ha accolto il ricorso nel il quale si affermava che la e-mail inviata da una ditta debitrice, nella quale si assicura il pagamento in tempi stretti della somma dovuta, può essere considerata prova scritta di promessa unilaterale di pagamento.

Secondo il ricorso l'e mail costituisce un documento informatico sottoscritto con firma elettronica "leggera", in quanto il mittente, per poter creare ed inviare detta e mail, dovrebbe eseguire un'operazione di validazione, inserendo il proprio username e la propria password.

Osserva infatti il ricorrente che" *Il documento informatico si può quindi definire sottoscritto con "firma elettronica" - cd. "semplice", per distinguerla dalla firma "digitale", che è un particolare tipo di firma elettronica qualificata che garantisce una maggiore autenticità e, di conseguenza, valore di scrittura privata autenticata, ex artt. 1, primo comma, lett. n) e 10, comma 3 del DPR 445/2000 - quando sia ricollegabile a qualsiasi metodo di "validazione" (cioè riconoscimento)*".
E ancora "*Per tali motivi, è pacifico che l'email costituisca un documento informatico sottoscritto con firma elettronica, in quanto il mittente, per poter creare ed inviare detta email, deve eseguire un'operazione di validazione, inserendo il proprio username e la propria password; e tale documento soddisfa altresì il requisito legale della forma scritta, a norma del combinato disposto degli artt. 1, primo comma, lett. cc) e 10, comma 2 del DPR 445/2000*".
Nell'ipotesi di opposizione al decreto ingiuntivo inizierà un procedimento ordinario nel quale il giudice, con sentenza, potrà accogliere la tesi del ricorso o potrà ritenerla non fondata.
Si allegano il testo del decreto e i primi commenti allo stesso, a cura dell'avv. Andrea Lisi (altalex) e a cura di Manlio Cammarata e Enrico Maccarone (interlex).

Successivamente altri giudici si sono pronunciati sul valore giuridico dell'e-mail. Si segnalano: decreto ingiuntivo del tribunale di Bari n. 89 dell'11 febbraio 2004; decreto ingiuntivo del tribunale di Mondovì n. 375 del 7 giugno 2004; decreto ingiuntivo del tribunale di Lucca dell'11 luglio 2004; decreto ingiuntivo del giudice di pace di Pesaro n. 598 del 2 febbraio 2004, ordinanza del tribunale di ancona del 9 aprile 2005.

Si allega il ricorso per decreto ingiuntivo, il decreto ingiuntivo e un commento sul valore probatorio dell'e- mail.

TRIBUNALE DI CUNEO

RICORSO PER DECRETO INGIUNTIVO

La AA S.r.l., corr. in MM (CN), in persona del legale rappresentante XX, elettivamente domiciliata in Cuneo presso l'Avv. Marco Cuniberti, dal quale è rappresentata per procura a margine del presente atto,

ESPONE

1) E' creditrice nei confronti della BB S.r.l., corr. in Novara, della complessiva somma di 2.593,36 per precedenti prestazioni e forniture.
2) Con email in data 20.10.2003 (di cui si produce copia, docc. 1 e 7), detta BB, in persona del legale rappresentante YY, riscontrò la lettera raccomandata di diffida Avv. Cuniberti 04.09.2003 (di cui si produce copia, doc. 2), assicurando espressamente il pagamento di quanto dovuto, entro la scadenza del 30.10.2003.
3) Diversamente da quanto promesso, la ditta debitrice non pagò (né alla scadenza indicata, né successivamente) il proprio debito.

4) Ad un nuovo sollecito dell'Avv. Cuniberti in data 03.11.2003 (di cui si produce copia, docc. 3 e 7), la

suddetta debitrice rispose (con email di cui si produce copia, docc. 4 e 7) lo stesso giorno, dichiarando addirittura (falsamente) di aver già pagato tramite bonifico bancario.
5) A nulla valse l'ulteriore diffida in data 11.11.2003 (di cui si produce copia, docc. 5 e 7), che, benchè regolarmente ricevuta in data 18.11.2003 (v. copia ricevuta, docc. 6 e 7), non ottenne più alcun riscontro: la debitrice non ha infatti a tutt'oggi pagato alcunchè all'esponente, costringendo quest'ultima alla presente azione giudiziale.
Sussistenza dei requisiti ex artt. 634 c.p.c.
6) La prodotta email inviata dalla debitrice in data 20.10.2003 ben costituisce una promessa unilaterale in forma di scrittura privata.
7) Sotto il primo aspetto, non vi son dubbi che il contenuto di detta missiva rappresenti una promessa di pagamento e/o una ricognizione di debito, specialmente se posta in relazione con la successiva dichiarazione 03.11.2003 (in cui la stessa debitrice dichiarò addirittura di aver già pagato).
8) Per quanto invece riguarda la richiesta forma ex art. 2702 c.c., occorre invece rifarsi al T.U. (D.P.R.) 445/2000 (così come modificato dal D.Lgs. 23 gennaio 2002, n. 10, dalla legge 16 gennaio 2003, n. 3 e dal D.P.R. 7 aprile 2003, n.137).
Ai sensi dell'art. articolo 1, primo comma, lett. b), il documento informatico è "la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti": l'email quindi, con il suo contenuto, rappresenta senza dubbio un documento informatico
8) Il successivo art. 8 stabilisce la piena validità giuridica di tale documento, disponendo che " "il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del presente testo unico".
9) L'art. 10, comma 2, prescrive poi che "Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta" (benchè con valore probatorio liberamente valutabile dal Giudice: ma questo non riguarda la fase monitoria, bensì, al limite, l'eventuale fase di merito); per quanto riguarda la definizione ed il significato di firma elettronica, occorre ritornare all'art. 1, comma primo, lett. cc) (relativo appunto alle definizioni), a norma del quale essa è "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica".
10) Il documento informatico si può quindi definire sottoscritto con "firma elettronica" - cd. "semplice", per distinguerla dalla firma "digitale", che è un particolare tipo di firma elettronica qualificata che garantisce una maggiore autenticità e, di conseguenza, valore di scrittura privata autenticata, ex artt. 1, primo comma, lett. n) e 10, comma 3 del DPR 445/2000 - quando sia ricollegabile a qualsiasi metodo di "validazione" (cioè riconoscimento): mentre nel mondo reale il metodo di validazione informatica più usato è costituito dal sistema "scheda magnetica + password (cioè un codice segreto, come ad esempio il sistema Bancomat)", per quanto riguarda internet, il procedimento più semplice e maggiormente utilizzato in tal senso è rappresentato dall'inserimento nel sistema in cui si vuole accedere di "username (cioè l'identificativo dell'utente) + password", che l'utente deve appunto digitare negli appositi spazi. Ed è proprio quanto avviene per la posta elettronica: per poter accedere ad un dato indirizzo (come quello utilizzato dalla debitrice) per inviare o controllare se si sono ricevute email, occorre conoscere ed inserire i suddetti dati identificativi (oppure utilizzare programmi - quale ad esempio Microsoft OUTLOOK EXPRESS - che inseriscono automaticamente tali dati ogni volta che ci si connette alla rete internet), procedendo quindi alla necessaria procedura di validazione.
11) Per tali motivi, è pacifico che l'email costituisca un documento informatico sottoscritto con firma elettronica, in quanto il mittente, per poter creare ed inviare detta email, deve eseguire un'operazione di validazione, inserendo il proprio username e la propria password; e tale documento soddisfa altresì il requisito legale della forma scritta, a norma del combinato disposto degli artt. 1, primo comma, lett. cc) e 10, comma 2 del DPR 445/2000.
12) Pertanto, poiché le prodotte email (contenenti la promessa unilaterale della debitrice) soddisfano il requisito della forma scritta, nel caso di specie ricorrono tutti i presupposti di legge per la concessione del decreto ingiuntivo.

Per i suesposti motivi, l'esponente

CHIEDE

alla S.V. Ill.ma di voler emettere, ai sensi degli artt. 633 e seguenti c.p.c., ingiunzione di pagamento a

carico della BB S.r.l., in persona del suo legale rappresentante, con sede in Novara, ……., a favore dell'esponente, della somma di 2.593,36, con gli interessi dalla domanda al saldo, nonché le spese giudiziali.
Ai fini della determinazione del contributo unificato, si precisa che l'importo della domanda è superiore a 1.033,00 ed inferiore a 5.165,00.
Produce:
1) Copia email YY 20.10.2003;
2) Copia raccomandata Avv. Cuniberti 04.09.2003
3) Copia email Avv. Cuniberti 03.11.2003;
4) Copia email YY 03.11.2003;
5) Copia email Avv. Cuniberti 11.11.2003;
6) Copia email YY 18.11.2003;
7) CD-ROM contenente i documenti informatici di cui ai precedenti docc. 1), 3), 4), 5) e 6).
8) Visura camerale BB S.r.l..
Cuneo, li 11 Dicembre 2003
Depositato in Cancelleria il 12.12.2003
Il Cancelliere
IL GIUDICE DESIGNATO DEL TRIBUNALE DI CUNEO
Visto il ricorso che precede
Ritenuta la propria competenza;
Visti gli artt. 633, 634 e 641 c.p.c.
INGIUNGE
Alla BB S.r.l., in persona del suo legale rappresentante, con sede in Novara, …., di pagare alla AAI S.r.l., CORR. IN MM……., la somma di 2.593,36, oltre gli interessi dalla data della domanda al saldo, nonché le spese di questo procedimento liquidate in ……(+ I.V.A. e C.P.A.), il tutto nel termine di giorni quaranta dalla notifica del presente decreto, avvertendo esso debitore che ha diritto di proporre opposizione avanti questo Tribunale nel medesimo termine di giorni quaranta e che, in mancanza di opposizione, si procederà esecutivamente.
Cuneo,
Il Giudice
Il Cancelliere
Depositato in Cancelleria il 15.12.2003

L'e-mail dal commercio elettronico alle aule di giustizia*

avv. Andrea Lisi
(Direttore Scientifico del Corso di Alta Formazione post-graduate in Diritto&Economia del Commercio Elettronico Internazionale – www.scint.it/altaformazione - Curatore del Portale per l'ICT & Internazionale Trade – www.scint.it)

Torniamo a trattare in questa nostra rubrica della validità ed efficacia della firma elettronica (se ne è già parlato nel n. 306 del 24/30 novembre 2003). Ce ne dà motivo il Tribunale di Cuneo che ha emesso, in data 15.12.2003, un decreto ingiuntivo (n. 848/03) condannando una società XX al pagamento di un credito vantato da altra società YY e fatto valere in giudizio sulla base del contenuto di alcune e.mail intercorse in precedenza tra le parti stesse (notizia apparsa sul sito giuridico Studium Fori all'indirizzo www.studiumfori.it/visallex.php?id=1474).
Il provvedimento in parola è di particolare interesse rappresentando un prima (se non addirittura la prima) pronuncia di un Giudice italiano sul complesso ed articolato tema della validità e producibilità in giudizio dei documenti informatici. L'argomentare del Tribunale di Cuneo, che per taluni aspetti appare condivisibile, rappresenta di certo uno stimolo per ulteriori riflessioni e studi da parte di quanti hanno a cuore le conseguenze giuridiche connesse alla diffusione delle nuove tecnologie informatiche.
Il nocciolo della questione si traduce in questo: l'e.mail è un documento informatico sprovvisto di qualsivoglia firma elettronica e perciò equivalente ad una mera riproduzione meccanica, ovvero è un documento informatico provvisto di firma elettronica almeno "leggera" soddisfacendo, così, il requisito della forma scritta?
Il controverso e dibattuto quadro normativo nazionale di riferimento è rappresentato dal Testo Unico (D.P.R.) 445/2000 (così come modificato dal D.Lgs. 23 gennaio 2002, n. 10, dalla legge 16 gennaio 2003,

n. 3 e dal D.P.R. 7 aprile 2003, n.137) a tenore del quale, tra l'altro, la firma elettronica è "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica*" (art. 1, comma primo, lett.c). In parole più semplici, si ha un documento informatico provvisto di firma elettronica *leggera* nel momento in cui dati elettronici connessi tra loro rendono in qualche modo "riconoscibili" le parti; riconoscibili quindi, attraverso metodi di *autenticazione informatica* - trattasi cioè dell' *insieme degli strumenti elettronici e delle procedure per la verifica indiretta dell'identità*, secondo la definizione fornita dal D.Lgs. 196/2003 all'art. 4 comma 3 lett. c) - quali ad esempio, l'uso di *password* o di codici di identificazione personale.
Secondo le argomentazioni poste a sostegno del ricorso presentato dall'avv. Marco Cuniberti, e quindi confermate dal Tribunale di Cuneo, non si dovrebbero nutrire dubbi nel considerare una e.mail alla stregua di un documento informatico provvisto di firma elettronica *leggera* dal momento che quella connessione biunivoca richiesta dalla legge, e a cui abbiamo innanzi accennato, ben si realizza con l'invio di una *missiva* di tal genere. Infatti, "per poter accedere ad un dato indirizzo (come quello utilizzato dalla debitrice) per inviare o controllare se si sono ricevute email, occorre conoscere ed inserire i suddetti dati identificativi (oppure utilizzare programmi - quale ad esempio Microsoft OUTLOOK EXPRESS - che inseriscono automaticamente tali dati ogni volta che ci si connette alla rete internet), procedendo quindi alla necessaria procedura di validazione"; e ciò sembrerebbe, alla luce della normativa (e in attesa di ulteriori modifiche) sufficiente a soddisfare la sottoscrizione con firma elettronica leggera e, quindi, il requisito della forma scritta.
Sarà poi compito del giudice valutare il valore probatorio di tale documento in giudizio e verificarne, quindi, la genuinità e riconducibilità effettiva del suo contenuto al titolare dell'indirizzo mail utilizzato. E, infatti, la normativa in oggetto attribuisce la validità di *forma scritta* al documento provvisto di semplice firma elettronica (*leggera*) e non al solo documento provvisto di firma elettronica avanzata (e, cioè, quel documento provvisto di *firma elettronica ottenuta attraverso una procedura informatica che garantisca la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati*).
Nel caso di specie il Giudice di Cuneo sulla base del contenuto di alcune e.mail (ed, in verità, anche sulla base di ulteriore documentazione a sostegno della posizione della società ricorrente) ha emesso il provvedimento in parola.
Facciamo largo, quindi, ai messaggi di posta elettronica nei giudizi? Probabilmente sì e non ci resta che aspettare ulteriori pronunce giurisdizionali.
Fin da ora, comunque, possiamo dire che il notevole successo della posta elettronica, anche nel mondo degli affari, ha determinato un fenomeno di massa che non può né deve rimanere privo di una regolamentazione di tipo legislativo.
Bene ha fatto dunque il Giudice di Cuneo ad accettarne la sua produzione in giudizio (d'altronde sin dalla lontana Bassanini bis - art. 15 secondo comma L. n. 59/97 - *gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonchè la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge*) e, forse, anche a considerare l'e.mail alla stregua di un documento provvisto di firma elettronica leggera e, quindi, ad attribuirle implicitamente *il requisito legale della forma scritta*; la sua pronuncia certamente contribuisce a rendere il mondo della rete più "reale". Così, se nel commercio elettronico (anche e soprattutto internazionale) abbiamo oramai abbandonato penne e francobolli per usare un pc connesso in rete, non dobbiamo dimenticare che tutto ciò che si poteva o non si poteva scrivere con la *semplice* penna lo si può o non lo si può scrivere con una *semplice* e.mail.
Da ciò consegue una considerazione più generale. Osservando l'evolversi della globalizzazione dei mercati, dell'allargamento delle frontiere e dell'intrecciarsi degli scambi commerciali internazionali (fenomeni addebitabili non certo alla sola evoluzione di Internet, ma precedenti alla stessa nascita della Rete) non si può non evidenziare come la legislazione sulla firma "digitale" appaia un po' in controtendenza rispetto alle politiche legislative sopranazionali, almeno per quanto concerne l'angolo di osservazione del giurista attento alle tematiche del diritto commerciale internazionale.
Nel Commercio Internazionale il legislatore sopranazionale è da sempre intervenuto per regolamentare delle prassi già consolidate, anche *servendosi* del potere "codificatore" di altre organizzazioni internazionali, quali la IIC (*International Chamber of Commerce*). Tale fenomeno lo si osserva, per fare soltanto qualche esempio, con gli *Incoterms*, con i *crediti documentari,* con le *lettere d'intenti,* con i *contratti-standard internazionali* e negli stessi *arbitrati internazionali,* ma anche in convenzioni internazionali di largo respiro (quali la Convenzione di Vienna del 1980) o negli stessi Pirncipi Unidroit.

Con l'avvento di Internet e del commercio elettronico (intrinsecamente internazionale), invece, la corsa forsennata verso una stretta regolamentazione di ogni singola realtà tecnologica lascia a volte senza parole, anzi per meglio dire senza fiato (considerando gli sforzi necessari a noi giuristi per star dietro a questa copiosa, complessa, contraddittoria evoluzione legislativa).
Il legislatore ha voluto imporre alla prassi l'utilizzo di alcuni particolari strumenti "*inventati" ad hoc* (quali la "*vecchia* firma digitale"), ovviamente senza riuscirci (almeno sino ad oggi).
Effettivamente le esigenze nuove di sicurezza e di imputabilità giuridica dello scambio telematico internazionale necessitano di particolare attenzione, ma almeno negli "affari tra privati" non sarebbe più giusto (come è già stato in passato) affidarsi al potere di una necessaria autoregolamentazione? Non sarebbe più normale guardare quel che succede negli affari telematici e cercare di intervenire con delle piccole correzioni giuridiche su quelle prassi piuttosto che mirare ad imporre nuovi strumenti mai utilizzati nell'e-commerce?
A mio avviso ciò che ha un senso nei rapporti tra Pubbliche Amministrazioni e tra Pubbliche Amministrazioni e privati non necessariamente deve avere un senso nei rapporti "più liberi" tra privati… e per tali motivi questo decreto ingiuntivo dovrebbe forse far aprire un po' gli occhi a chi continua a desiderare stringenti regolamentazioni tecniche anche in aree di scambio da sempre affidate alla libera creatività dei loro protagonisti.
* *Un estratto del presente articolo sarà pubblicato nella Rubrica "Diritto & Internet" curata dall'avv. Andrea Lisi e ospitata settimanalmente nel Corriere delle Telecomunicazioni, ed. Edicomp Holding S.p.A. , Roma*

Un messaggio e-mail non è "prova scritta"

di Manlio Cammarata e Enrico Maccarone - 29.01.04

Circola in questi giorni sul web la strana notizia di una decisione del tribunale di Cuneo, nella quale il giudice avrebbe sentenziato che l'e-mail ha l'efficacia probatoria di una scrittura privata. In questo modo sarebbe confermata una strana interpretazione della normativa sulla firma digitale: l'inserimento della password per accedere al servizio di posta costituirebbe una firma elettronica. Interpretazione insostenibile, come vedremo tra poco, anche sulla base di una attenta lettura delle norme.
Il fatto è che la notizia non sta in piedi. Il testo in questione, come si può vedere dal documento che pubblichiamo, è un ricorso per decreto ingiuntivo. Tutto il bailamme di commenti più o meno appropriati che si stanno intrecciando sulla presunta "sentenza", in realtà è fondato sul nulla. Non c'è alcuna sentenza da commentare. In ipotesi, nell'eventuale giudizio di opposizione al decreto ingiuntivo, la sentenza del tribunale potrebbe accogliere la tesi contraria a quella sostenuta dal ricorrente. Ipotesi non peregrina, perché di solito i giudici sanno leggere le norme meglio di molti improvvisati commentatori.
Per essere più chiari:
1. L'oggetto della discussione non è una sentenza, ma solo il ricorso di una parte al giudice. Sono dunque argomentazioni di parte, che in nessun caso possono costituire "giurisprudenza".
2. Un decreto ingiuntivo non è una sentenza. L'art. 633 del codice di procedura civile dice che il giudice emette il decreto "se del diritto fatto valere si dà prova scritta", ma anche "se il diritto dipende da una controprestazione o da una condizione, purché il ricorrente offra elementi atti a far presumere l'adempimento della controprestazione o l'avveramento della condizione". Non possiamo sapere se il giudice ha ritenuto di accogliere le argomentazioni del ricorrente sull'attribuzione dell'efficacia di "forma scritta" alle e-mail, o abbia trovato nelle stesse e-mail gli "altri elementi" previsti dal codice di procedura civile: un decreto ingiuntivo, per sua natura, non contiene motivazioni.
3. Chi pretende di commentare un atto di parte come se fosse una sentenza e lo porta a sostegno delle proprie tesi, non ha idee chiare in materia di diritto.
Ciò premesso, dobbiamo approfondire la sostanza della questione: l'inserimento del nome dell'utente e della password per accedere ai servizi del provider che ospita la casella di posta del mittente è una "firma elettronica" ai sensi della normativa vigente?
Il problema è serio, perché da qualche tempo circola questa interpretazione, fondata su apparenti giustificazioni tecniche, non giuridiche, che può avere conseguenze devastanti. Ne avevamo già parlato qualche tempo fa in una FAQ sulla firma digitale ma, vista la situazione, è necessario ritornare sull'argomento in maniera più esaustiva.

Le argomentazioni addotte dall'avvocato del ricorrente sembrano seguire una ferrea concatenazione logica. Ma sono viziate in partenza da una superficiale considerazione del dato normativo o, più esattamente, da una mancanza di collegamento tra il dato normativo e il dato di fatto. Per dirla in termini più semplici, si dà della norma una lettura che non corrisponde alla realtà, anche per il semplice fatto che la norma stessa, nella sua attuale formulazione, si presta a interpretazioni errate o devianti.
In sostanza, afferma il ricorrente, un messaggio e-mail è una "scrittura privata", dal momento che l'art. 10, comma 2, del DPR 445/2000 stabilisce che "Il documento informatico, sottoscritto con firma elettronica, soddisfa il requisito legale della forma scritta". Allora ci si deve chiedere dov'è la firma elettronica in un messaggio e-mail (a parte la probabile incostituzionalità di questa disposizione, per i motivi che abbiamo più volte esposto in queste pagine - vedi, in particolare, Lo schema governativo stravolge il processo civile di Gianni Buonomo e La Costituzione, la delega e le "disarmonie" del testo di Daniele Coliva).
Secondo la tesi del ricorrente, condivisa da alcuni distratti commentatori, la firma elettronica sarebbe costituita dal nome dell'utente e dalla password immessi per accedere al server del provider di posta elettronica. E questo è l'errore.
Leggiamo punto per punto la definizione di "firma elettronica", nel testo vigente del DPR 445/00, art. 1,comma, 1, lettera cc):
- *l'insieme dei dati in forma elettronica,*
- *allegati oppure connessi tramite associazione logica ad altri dati elettronici,*
- *utilizzati come metodo di autenticazione informatica*.

Nessun dubbio che nome utente e password costituiscano un insieme di dati in forma elettronica, ma si deve aggiungere il secondo punto: questi dati devono essere "allegati oppure connessi tramite associazione logica" ad altri dati elettronici, che sono appunto quelli che devono essere validati. L'efficacia materiale di quei dati informatici, che la direttiva 1999/93/CE definisce impropriamente "firma elettronica", deriva appunto dal fatto che c'è una connessione logica tra i dati "validanti" e i dati che devono essere validati. Connessione logica che avviene attraverso la procedura - logica - che calcola l'impronta dei dati da validare e la cifra con la chiave privata del firmatario.
In mancanza di questa procedura, o di un'altra che abbia il medesimo effetto, non si può parlare di qualsivoglia forma di firma elettronica, perché manca l'associazione logica tra il dato validante e il dato validato. L'immissione di dati quali userid e password nella fase iniziale di accesso al server non comporta alcuna associazione logica tra questi dati e gli altri dati elettronici che costituiscono i messaggio e-mail. Sarebbe come affermare che quando si deve inserire una password per accedere a un PC, tutti i documenti contenuti in quella macchina hanno la firma elettronica.
In conclusione:
a) sul piano del diritto non vi è alcun elemento per affermare che l'accesso con userid e password al servizio e-mail possa configurare la firma elettronica dei documenti inviati.
b) sul piano del fatto è fin troppo facile far apparire un'identità fittizia come mittente dell'e-mail; tanto che molti di quelli che ritengono che dalle norme si possa evincere la natura di firma elettronica per userid e password, finiscono col chiedersi se le norme stesse non siano sbagliate.
Tutto questo conferma quanto andiamo scrivendo da tempo: è indispensabile e urgente rivedere la normativa sul documento informatico, partendo dalle definizioni: le direttive comunitarie non devono essere "copiate" dagli Stati membri, ma "attuate". La differenza tra "copia" e "attuazione" è fin troppo evidente per giustificare ulteriori considerazioni.

In Gazzetta Ufficiale la direttiva per l'impiego della posta elettronica nelle pubbliche amministrazioni

NUMERO SCHEDA: 4192

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: POSTA ELETTRONICA

FONTE: GAZZETTA UFFICIALE

NUMERO: 8

DATA: 12/01/2004

PAGINA: 14 ss

RIFERIMENTO NORMATIVO: l. 229/2003; d.p.r. 445/2000

NATURA ATTO: DIRETTIVA

DATA ATTO: 27/11/2003

ORGANO: MINISTERI

SCHEDE COLLEGATE: 3892; 4049; 4178; 4189; 4285

Sulla Gazzetta Ufficiale n. 8 del 12 gennaio 2004 è stata pubblicata la direttiva del Ministro per l'Innovazione e le Tecnologie del 27 novembre 2003 sull'impiego della posta elettronica nelle pubbliche amministrazioni, articolata in 3 paragrafi.
Nel paragrafo I, dopo il richiamo alle "Linee guida per lo sviluppo della società dell'informazione nella legislatura", approvate dal Consiglio dei ministri il 31 maggio 2002, si evidenzia come 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*" e si sottolinea la necessità di tempi rapidi per l'attuazione completa del processo di informatizzazione della pubblica amministrazione.
Nel paragrafo II si segnala che, per una piena attuazione del disposto di cui all'art. 14 del d.p.r. 445/2000 (sull'utilizzo della posta elettronica da parte della P.A.), è necessario che tutti i dipendenti abbiano una casella di posta elettronica e che le pubbliche amministrazioni attivino apposite caselle istituzionali affidate alla responsabilità delle strutture di competenza (con conseguente lettura della corrispondenza almeno una volta al giorno).
Sempre al paragrafo II della direttiva, sotto la voce "caratteristiche", si evidenziano i vantaggi della posta elettronica rispetto ai tradizionali mezzi di comunicazione (semplicità, economicità, velocità, ecc.).
Nei "contenuti" si afferma che le pubbliche amministrazioni si adopereranno per estendere l'uso della posta elettronica (utilizzabile per molteplici e diverse tipologie di atti) e si ribadisce che tutti i dipendenti dovranno essere dotati di una casella di posta elettronica.
Nel paragrafo III si rammenta che il Comitato dei Ministri per la societa' 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.

Si allega il testo della direttiva.

Dir.Min. 27 novembre 2003
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'art. 14 del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, approvato con decreto del Presidente della Repubblica 28 dicembre 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'àmbito 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 nella 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.
È, 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'àmbito 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.

Pubblicato sulla Gazzetta Ufficiale il decreto ministeriale in materia di posta elettronica certificata.

NUMERO SCHEDA: 6804

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: POSTA ELETTRONICA

NATURA ATTO: DECRETO MINISTERIALE

E' stato pubblicato nella G.U. del 15 novembre 2005, n. 266 il Decreto Ministeriale recante le "Regole tecniche del servizio di trasmissione di documenti informatici mediante la posta elettronica certificata" che definisce i requisiti tecnico–funzionali previsti per l'erogazione del servizio. Con la pubblicazione in G.U. del decreto, si completa il quadro normativo di riferimento per la Posta Elettronica Certificata. Nei prossimi giorni inoltre verrà pubblicata in Gazzetta anche la Circolare Cnipa che definisce le modalità di accreditamento all'elenco pubblico dei gestori. Si apre in tal modo la possibilità, per gli operatori di mercato in possesso dei requisiti previsti dalla legge, di qualificarsi quali gestori di Posta Elettronica Certificata.

Si allega il comunicato stampa del Cnipa e, di seguito, il testo integrale del decreto ministeriale.

L'Italia è il primo paese d'Europa a disporre di un servizio di posta elettronica certificata, ossia di "raccomandata elettronica", regolato da legge. Con la pubblicazione, domani lunedì, nella Gazzetta Ufficiale del decreto firmato da Lucio Stanca, ministro per l'Innovazione e le Tecnologie, si completa infatti il complesso quadro normativo che consentirà ai gestori di avviare all'operatività questo innovativo servizio.
"È stato compiuto un importante passo in avanti per rendere sempre più veloce, sicuro, comodo ed economico l'invio di documenti importanti mediante le nuove tecnologie digitali, semplificando così la vita di cittadini ed imprese nell'ambito del più vasto processo di modernizzazione del Paese attualmente in atto con un impiego di risorse senza precedenti", ha detto il ministro Stanca, ricordando poi che "questo strumento dà validità giuridica ai documenti inoltrati per posta elettronica agli uffici pubblici o privati".
Da parte sua Livio Zoffoli, presidente del CNIPA, organismo che è gestore e punto di riferimento di questa rivoluzione postale, ha spiegato che "la peculiarità della 'raccomandata elettronica' rispetto a quella tradizionale, cartacea, sta non solo nella tempestività dell'inoltro, in qualsiasi ora del giorno e da qualunque luogo ove sia possibile collegarsi ad una rete telematica, ma anche e soprattutto nel fatto che essa consente di avere sul proprio pc, la ricevuta di ricezione non soltanto della busta, ma anche del suo contenuto".
Dopo il regolamento relativo alle disposizioni per l'utilizzo della posta elettronica certificata, pubblicato nel febbraio scorso, l'ultimo provvedimento firmato da Stanca definisce le regole tecniche relative alle modalità di realizzazione e di funzionamento della "PEC" ed è accompagnato da un allegato tecnico che sarà consultabile on line nel sito del CNIPA. Il Centro Nazionale per l'Informatica, oltre a verificare in funzione dell'evoluzione tecnologica la coerenza operativa degli standard adottati nelle specifiche tecniche, ha già predisposto una circolare di accreditamento per i gestori con le indicazioni sia dei documenti che dovranno presentare per poter operare il servizio, sia della struttura organizzativa, dell'organizzazione del servizio, del manuale operativo e di sicurezza e, non ultimi, dei livelli minimi di qualità del servizio erogato (tra cui l'interruzione massima consentita per il servizio o i termini temporali per gli avvisi di mancata consegna).
Il cittadino o l'impresa che invierà un messaggio di posta elettronica certificata avrà ben due conferme: una relativa alla ricevuta accettazione dell'inoltro effettuato; un'altra di avvenuta consegna della comunicazione e degli allegati. I messaggi vengono consegnati inalterati inseriti all'interno di un

messaggio (busta di trasporto) che ne garantisce l'integrità e ne permette i controlli di provenienza. Tutte le operazioni sono tracciate e registrate.

IL MINISTRO
PER L'INNOVAZIONE E LE TECNOLOGIE

Decreta:

Capo I - Principi generali

1. Definizioni.

1. Ai fini del presente decreto si applicano le definizioni contenute nell'art. 1 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, citato nelle premesse. Si intende, inoltre, per:
a) punto di accesso: il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto;
b) punto di ricezione: il sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto;
c) punto di consegna: il sistema che compie la consegna del messaggio nella casella di posta elettronica certificata del titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna;
d) firma del gestore di posta elettronica certificata: la firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del gestore.
e) ricevuta di accettazione: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata;
f) avviso di non accettazione: l'avviso, sottoscritto con la firma del gestore di posta elettronica certificata del mittente, che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non è possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario;
g) ricevuta di presa in carico: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata del mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce;
h) ricevuta di avvenuta consegna: la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio è inserito nella casella di posta elettronica certificata del destinatario;
i) ricevuta completa di avvenuta consegna: la ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale;
l) ricevuta breve di avvenuta consegna: la ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale;
m) ricevuta sintetica di avvenuta consegna: la ricevuta che contiene i dati di certificazione;
n) avviso di mancata consegna: l'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario;
o) messaggio originale: il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene;

p) busta di trasporto: la busta creata dal punto di accesso e sottoscritta con la firma del gestore di posta elettronica certificata del mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione;
q) busta di anomalia: la busta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, nella quale è inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un titolare, per evidenziare al destinatario detta anomalia;
r) dati di certificazione: i dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore di posta elettronica certificata del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto;
s) gestore di posta elettronica certificata: il soggetto che gestisce uno o più domini di posta elettronica certificata con i relativi punti di accesso, di ricezione e di consegna, titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari;
t) titolare: il soggetto a cui è assegnata una casella di posta elettronica certificata;
u) dominio di posta elettronica certificata: dominio di posta elettronica certificata che contiene unicamente caselle di posta elettronica certificata;
v) indice dei gestori di posta elettronica certificata: il sistema, che contiene l'elenco dei domini e dei gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata.
z) casella di posta elettronica certificata: la casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata ed alla quale è associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata;
aa) marca temporale: un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004.

2. Obiettivi e finalità.

1. Il presente decreto definisce le regole tecniche relative alle modalità di realizzazione e funzionamento della posta elettronica certificata di cui al decreto del Presidente della Repubblica n. 68 del 2005.

3. Norme tecniche di riferimento

1. Sono di seguito elencati gli standard di riferimento delle norme tecniche, le cui specifiche di dettaglio vengono riportate in allegato al presente decreto:
a) RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted);
b) RFC 1891 (SMTP Service Extension for Delivery Status Notifications);
c) RFC 1912 (Common DNS Operational and Configuration Errors);
d) RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions);
e) RFC 2315 (PKCS#7: Cryptographic Message Syntax Version 1.5);
f) RFC 2633 (S/MIME Version 3 Message Specification);
g) RFC 2660 (The Secure HyperText Transfer Protocol);
h) RFC 2821 (Simple Mail Transfer Protocol);
i) RFC 2822 (Internet Message Format);
l) RFC 2849 (The LDAP Data Interchange Format (LDIF) - Technical Specification);
m) RFC 3174 (US Secure Hash Algorithm 1 - SHA1);
n) RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security);
o) RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile).

4. Compatibilità operativa degli standard.

1. Il Centro nazionale per l'informatica nella pubblica amministrazione, di seguito denominato CNIPA, verifica, in funzione dell'evoluzione tecnologica, la coerenza operativa degli standard così come adottati nelle specifiche tecniche, dando tempestiva informazione delle eventuali variazioni nel proprio sito istituzionale.

Capo II - Disposizioni per i titolari e per i gestori di posta elettronica certificata

5. Comunicazione e variazione della disponibilità all'utilizzo della posta elettronica certificata.

1. La dichiarazione di cui all'art. 4, comma 4, del decreto del Presidente della Repubblica n. 68 del 2005, può essere resa mediante l'utilizzo di strumenti informatici, nel qual caso la dichiarazione deve essere sottoscritta con la firma digitale di cui all'art. 1, comma 1, lettera n) del decreto del Presidente della Repubblica n. 445 del 2000.
2. La dichiarazione di cui al comma 1 è resa anche nei casi di variazione dell'indirizzo di posta elettronica certificata o di cessazione della volontà di avvalersi della posta elettronica certificata medesima.

6. Caratteristiche dei messaggi gestiti dai sistemi di posta elettronica certificata.

1. I sistemi di posta elettronica certificata generano messaggi conformi allo standard internazionale S/MIME, così come descritto dallo standard RFC 2633.
2. I messaggi di cui al comma 1 si dividono in tre categorie:
a) ricevute;
b) avvisi;
c) buste.
3. La differenziazione dei messaggi, come indicato nel comma 2, è realizzata dai sistemi di posta elettronica certificata utilizzando la struttura header, prevista dallo standard S/MIME, da impostare per ogni tipologia di messaggio in conformità a quanto previsto dalle specifiche tecniche di cui all'allegato.
4. I sistemi di posta elettronica certificata in relazione alla tipologia di messaggio da gestire realizzano funzionalità distinte e specifiche.
5. L'elaborazione dei messaggi di posta elettronica certificata avviene anche nel caso in cui il mittente ed il destinatario appartengano allo stesso dominio di posta elettronica certificata.
6. Le ricevute generate dai sistemi di posta elettronica certificata sono le seguenti:
a) ricevuta di accettazione;
b) ricevuta di presa in carico;
c) ricevuta di avvenuta consegna completa, breve, sintetica.
7. La ricevuta di avvenuta consegna è rilasciata per ogni destinatario al quale il messaggio è consegnato.
8. Gli avvisi generati dai sistemi di posta elettronica certificata sono i seguenti:
a) avviso di non accettazione per eccezioni formali ovvero per virus informatici;
b) avviso di rilevazione di virus informatici;
c) avviso di mancata consegna per superamento dei tempi massimi previsti ovvero per rilevazione di virus informatici.
9. Le buste generate dai sistemi di posta elettronica certificata sono le seguenti:
a) busta di trasporto;
b) busta di anomalia.
10. La busta di trasporto è consegnata immodificata nella casella di posta elettronica certificata di destinazione per permettere la verifica dei dati di certificazione da parte del ricevente.

7. Firma elettronica dei messaggi di posta elettronica certificata.

1. I messaggi di cui all'art. 6, generati dai sistemi di posta elettronica certificata, sono sottoscritti dai gestori mediante la firma del gestore di posta elettronica certificata, in conformità a quanto previsto dall'allegato.

2. I certificati di firma di cui al comma 1 sono rilasciati dal CNIPA al gestore al momento dell'iscrizione nell'elenco pubblico dei gestori di posta elettronica certificata e sino ad un numero massimo di dieci firme per ciascun gestore.
3. Qualora un gestore abbia ravvisato la necessità di utilizzare un numero di certificati di firma superiore a dieci, può richiederli al CNIPA documentando tale necessità. Il CNIPA, previa valutazione della richiesta, stabilisce se fornire o meno al gestore ulteriori certificati di firma.

8. Interoperabilità.

1. Le specifiche tecniche finalizzate a garantire l'interoperabilità sono definite nell'allegato.

9. Riferimento temporale.

1. A ciascuna trasmissione è apposto un unico riferimento temporale, secondo le modalità indicate nell'allegato.
2. Il riferimento temporale può essere generato con qualsiasi sistema che garantisca stabilmente uno scarto non superiore ad un minuto secondo rispetto alla scala di tempo universale coordinato (UTC), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273.

10. Conservazione dei log dei messaggi.

1. Al fine della conservazione dei log dei messaggi, di cui alle deliberazioni del CNIPA in materia di riproduzione e conservazione dei documenti su supporto ottico, ogni gestore provvede a:
a) definire un intervallo temporale unitario non superiore alle ventiquattro ore;
b) eseguire senza soluzioni di continuità il salvataggio dei log dei messaggi generati in ciascun intervallo temporale come sopra definito.
2. Ai file generati da ciascuna operazione di salvataggio deve essere associata la relativa marca temporale.

11. Conservazione dei messaggi contenenti virus e relativa informativa al mittente.

1. Il gestore è tenuto a trattare il messaggio contenente virus secondo le regole tecniche indicate nell'allegato.
2. Il gestore è tenuto ad informare il mittente che il messaggio inviato contiene virus.
3. Il gestore è tenuto a conservare il messaggio contenente virus per un periodo non inferiore ai trenta mesi secondo le modalità indicate nelle deliberazioni del CNIPA in materia di riproduzione e conservazione dei documenti su supporto ottico.

12. Livelli di servizio.

1. Il gestore di posta elettronica certificata può fissare il numero massimo di destinatari e la dimensione massima del singolo messaggio, sia per i messaggi che provengono da un suo titolare, sia per i messaggi che provengono da titolari di caselle di altri gestori di posta elettronica certificata.
2. In ogni caso il gestore di posta elettronica certificata deve garantire la possibilità dell'invio di un messaggio:
a) almeno fino a cinquanta destinatari;
b) per il quale il prodotto del numero dei destinatari per la dimensione del messaggio stesso non superi i trenta megabytes.
3. La disponibilità nel tempo del servizio di posta elettronica certificata deve essere maggiore o uguale al 99,8% del periodo temporale di riferimento.
4. Il periodo temporale di riferimento, per il calcolo della disponibilità del servizio di posta elettronica certificata, è pari ad un quadrimestre.
5. La durata massima di ogni evento di indisponibilità del servizio di posta elettronica certificata deve essere minore, o uguale, al 50% del totale previsto per l'intervallo di tempo di riferimento.

6. Nell'àmbito dell'intervallo di disponibilità di cui al comma 3, la ricevuta di accettazione deve essere fornita al mittente entro un termine, da concordarsi tra gestore e titolare, da calcolare a partire dall'inoltro del messaggio, non considerando i tempi relativi alla trasmissione.
7. Al fine di assicurare in ogni caso il completamento della trasmissione ed il rilascio delle ricevute, il gestore di posta elettronica certificata descrive nel manuale operativo, di cui all'art. 23, le soluzioni tecniche ed organizzative che realizzano i servizi di emergenza, ai sensi di quanto previsto dall'art. 11, comma 4, del decreto del Presidente della Repubblica n. 68 del 2005, e consentano il rispetto dei vincoli definiti nei commi 4 e 5 del presente articolo.

13. Avvisi di mancata consegna.

1. Qualora il gestore del mittente non abbia ricevuto dal gestore del destinatario, nelle dodici ore successive all'inoltro del messaggio, la ricevuta di presa in carico o di avvenuta consegna del messaggio inviato, comunica al mittente che il gestore del destinatario potrebbe non essere in grado di realizzare la consegna del messaggio.
2. Qualora, entro ulteriori dodici ore, il gestore del mittente non abbia ricevuto la ricevuta di avvenuta consegna del messaggio inviato, inoltra al mittente un ulteriore avviso relativo alla mancata consegna del messaggio entro le 24 ore successive all'invio, così come previsto dal decreto del Presidente della Repubblica n. 68 del 2005.

14. Norme di garanzia sulla natura della posta elettronica ricevuta.

1. Il gestore di posta elettronica certificata del destinatario ha l'obbligo di segnalare a quest'ultimo se la posta elettronica in arrivo non è qualificabile come posta elettronica certificata, secondo quanto prescritto dal decreto del Presidente della Repubblica n. 68 del 2005, nonché dal presente decreto e relativo allegato.
2. I messaggi relativi all'invio e alla consegna di documenti attraverso la posta elettronica certificata sono rilasciati indipendentemente dalle caratteristiche e dal valore giuridico dei documenti trasmessi.

15. Limiti di utilizzo.

1. La pubblica amministrazione che intende iscriversi all'elenco dei gestori di posta elettronica certificata, di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005, è tenuta a presentare al CNIPA una relazione tecnica che illustri le misure adottate affinché l'utilizzo di caselle di posta elettronica rilasciate a privati dall'amministrazione medesima:
a) costituisca invio valido ai sensi dell'art. 16, comma 2, del decreto del Presidente della Repubblica n. 68 del 2005
b) avvenga limitatamente ai rapporti di cui al medesimo art. 16, comma 2.

16. Modalità di iscrizione all'elenco dei gestori di posta elettronica certificata.

1. I soggetti che presentano domanda di iscrizione all'elenco pubblico, di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005, forniscono inoltre al CNIPA le informazioni e i documenti di seguito indicati, anche su supporto elettronico, ad eccezione del documento di cui alla lettera e):
a) denominazione sociale;
b) sede legale;
c) sedi presso le quali è erogato il servizio;
d) rappresentante legale;
e) piano per la sicurezza, contenuto in busta sigillata;
f) manuale operativo di cui all'art. 23;
g) dichiarazione di impegno al rispetto delle disposizioni del decreto del Presidente della Repubblica n. 68 del 2005;
h) dichiarazione di conformità ai requisiti previsti nel presente decreto e suo allegato;
i) relazione sulla struttura organizzativa.
2. I soggetti che rivestono natura giuridica privata trasmettono, inoltre, copia cartacea di una polizza assicurativa o di un certificato provvisorio impegnativo di copertura dei rischi dell'attività e dei danni causati a terzi, rilasciata da una società di assicurazioni abilitata ad esercitare nel campo dei rischi industriali, a norma delle vigenti disposizioni.

17. Equivalenza dei requisiti dei gestori stranieri.

1. Il gestore di posta elettronica certificata stabilito in altri Stati membri dell'Unione europea che si trovi nelle condizioni di cui all'art. 15 del decreto del Presidente della Repubblica n. 68 del 2005 ed intenda esercitare il servizio di posta elettronica certificata in Italia, comunica in via preventiva al CNIPA tale intenzione ed ogni notizia utile al fine della verifica di cui al citato art. 15. La comunicazione costituisce domanda di iscrizione nell'elenco di gestori di posta elettronica certificata; sono applicabili le disposizioni procedimentali di cui all'art. l4 del decreto del Presidente della Repubblica n. 68 del 2005.

18. Indice ed elenco pubblico dei gestori di posta elettronica certificata.

1. I gestori di posta elettronica certificata si attengono alle regole riportate nell'allegato per accedere all'indice dei gestori di posta elettronica certificata.
2. Il certificato elettronico, da utilizzare per la funzione di accesso di cui al comma 1, è rilasciato dal CNIPA al gestore al momento dell'iscrizione nell'elenco pubblico di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005.
3. L'elenco pubblico dei gestori di posta elettronica certificata tenuto dal CNIPA contiene, per ogni gestore, le seguenti indicazioni:
a) denominazione sociale;
b) sede legale;
c) rappresentante legale;
d) indirizzo internet;
e) data di iscrizione all'elenco;
f) data di cessazione ed eventuale gestore sostitutivo.
4. L'elenco pubblico è sottoscritto con firma digitale dal CNIPA, che lo rende disponibile per via telematica.

19. Disciplina dei compiti del CNIPA.

1. Il CNIPA definisce con circolari le modalità di inoltro della domanda e le modalità dell'esercizio dei compiti di vigilanza e controllo di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005.

20. Sistema di qualità del gestore.

1. Entro un anno dall'iscrizione del gestore all'elenco pubblico di cui all'art. 14 del decreto del Presidente della Repubblica n. 68 del 2005, il gestore medesimo fornisce copia della certificazione di conformità del proprio sistema di qualità alle norme UNI EN ISO 9001:2000 e successive evoluzioni relativamente a tutti i processi connessi al servizio di posta elettronica certificata.
2. Il manuale della qualità è depositato presso il CNIPA e reso disponibile presso il gestore.

21. Organizzazione e funzioni del personale del certificatore.

1. L'organizzazione del personale addetto al servizio di posta elettronica certificata prevede almeno la presenza di responsabili preposti allo svolgimento delle seguenti attività e funzioni:
a) registrazione dei titolari;
b) servizi tecnici;
c) verifiche e ispezioni (auditing);
d) sicurezza;
e) sicurezza dei log dei messaggi;
f) sistema di riferimento temporale.
2. È possibile attribuire al medesimo soggetto più responsabilità tra quelle previste dalle lettere d), e) ed f).

22. Requisiti di competenza ed esperienza del personale.

1. Il personale cui sono attribuite le funzioni previste dall'art. 21 deve aver maturato un'esperienza almeno quinquennale nelle attività di analisi, progettazione, commercializzazione e conduzione di sistemi informatici.
2. Per ogni aggiornamento apportato al sistema di posta elettronica certificata, il gestore eroga, alle figure professionali interessate, apposita attività di addestramento.

23. Manuale operativo.

1. Il manuale operativo definisce e descrive le procedure applicate dal gestore di posta elettronica certificata nello svolgimento della propria attività.
2. Il manuale operativo è depositato presso il CNIPA.
3. Il manuale contiene:
a) i dati identificativi del gestore;
b) i dati identificativi della versione del manuale operativo;
c) l'indicazione del responsabile del manuale operativo;
d) l'individuazione, l'indicazione e la definizione degli obblighi del gestore di posta elettronica certificata e dei titolari;
e) la definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;
f) l'indirizzo del sito web del gestore ove sono pubblicate le informazioni relative ai servizi offerti;
g) le modalità di protezione della riservatezza dei dati;
h) le modalità per l'apposizione e la definizione del riferimento temporale.
Il presente decreto è inviato ai competenti organi di controllo ed è pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

Avvertenza:

Il testo dell'allegato al presente decreto del Ministro per l'innovazione e le tecnologie, recante «Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata», è pubblicato e consultabile sul sito telematico del CNIPA - Centro nazionale per l'informatica nella pubblica amministrazione http//www.cnipa.gov.it.

CAPITOLO V

PROTOCOLLO INFORMATICO

Il legislatore definisce il protocollo informatico come l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti, ovvero, tutte le risorse tecnologiche necessarie alla realizzazione di un sistema automatico per la gestione elettronica dei flussi documentali[1].

Ogni sistema di protocollo informatico, che si intende adottare o realizzare, deve ottemperare a specifiche indicazioni, riportate nel Testo Unico (DPR 445/2000).

L'attuale quadro normativo in materia di gestione informatica della documentazione amministrativa, pone il nostro paese all'avanguardia per le possibilità di innovazione e di miglioramento dei servizi della Pubblica Amministrazione.

Lo sviluppo degli strumenti quali la firma elettronica ed il protocollo informatico, integrati ai servizi di interoperabilità, rende possibile la realizzazione effettiva di una gestione completamente automatizzata dei flussi documentali e la conseguente attuazione di profonde innovazioni nelle modalità di lavoro delle amministrazioni e nei rapporti tra esse e i cittadini.

In particolare, i sistemi di protocollo informatico e di gestione dei flussi documentali, possono diventare lo strumento che abilita la completa attuazione della trasparenza amministrativa tra amministrazioni e cittadini e imprese, intesa come concreto diritto del cittadino e dell'impresa di conoscere lo stato delle attività amministrative che li riguardano e avere la garanzia che tali attività siano condotte nel rispetto di regole di priorità e massimo impegno.

Sono tenuti a realizzare la gestione del protocollo con sistemi informativi automatizzati le pubbliche amministrazioni indicate nel decreto legislativo 30 marzo 2001, n. 165, che sono: "tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le regioni, le province, i comuni, le comunità

---

2 *L'introduzione al capitolo relativo al protocollo informatico è tratta dalla sezione dedicata all'argomento del sito http://protocollo.gov.it/. La scelta è dovuta alla chiarezza espositiva con la quale viene introdotto un argomento che presenta problematiche tecniche di non immediata comprensione.*

montane, e loro consorzi ed associazioni, le istituzioni universitarie, gli istituti autonomi case popolari, le camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale".

Ogni Pubblica Amministrazione, perseguendo gli obiettivi previsti dal proprio mandato istituzionale, riceve e produce una enorme quantità di documenti.

Tale attività si estrinseca in processi governati da procedure e regole variabilmente complesse ed articolate.

L'attività di protocollazione è quella fase del processo che certifica provenienza e data di acquisizione del documento identificandolo in maniera univoca nell'ambito di una sequenza numerica collegata con l'indicazione cronologica. Costituisce pertanto il punto nevralgico di tutti i flussi di lavoro tra le Amministrazioni ed all'interno di ciascuna di esse; le modalità di gestione adottate in merito assumono di conseguenza una importanza fondamentale nella strategia operativa della Pubblica Amministrazione.

Inoltre, la memoria relativa ad attività svolte (se necessaria ai bisogni amministrativi degli individui e, ancor più, delle strutture, alla programmazione delle attività future) richiede organizzazione, nel caso specifico un inquadramento nel tempo e nello spazio dei documenti prodotti e conservati e il collegamento con le attività a cui partecipano.

Gli obiettivi che si vogliono raggiungere con lo strumento "protocollo informatico" sono fondamentalmente due: in primo luogo rendere maggiormente efficienti le amministrazioni - attraverso l'eliminazione dei registri cartacei, la diminuzione degli uffici di protocollo, la razionalizzazione dei flussi documentali - e secondariamente migliorare la trasparenza dell'azione amministrativa attraverso strumenti che rendano possibile un effettivo esercizio del diritto di accesso allo stato dei procedimenti e ai relativi documenti da parte dei soggetti interessati (cittadini e imprese).

La strategia seguita, dall'Autorità per l'informatica nella pubblica amministrazione prima e dal Ministro per l'innovazione e le tecnologie poi, sul tema è stata quella di emanare delle norme comuni (DPR 428/98 poi confluito nel DPR 445/2000) per la salvaguardia della trasparenza amministrativa (per garantire, ad esempio, la non modificabilità delle registrazioni, oppure la stretta sequenzialità della

numerazione dei documenti), lasciando alla autonomia di ciascuna amministrazione tutti gli aspetti relativi al miglioramento della propria efficienza interna - come la scelta sull'organizzazione del flusso interno di lavorazione dei documenti e sul livello di automazione attuabile.

Allo scopo di dare impulso alla realizzazione dei sistemi di protocollo informatico e conseguentemente a progetti volti alla trasparenza dell'azione amministrativa il Governo ha istituito presso il Dipartimento per l'Innovazione e le Tecnologie un Project Office composto da esperti della materia per il coordinamento delle attività di dispiegamento del progetto nella P.A. centrale e locale.

L'attuazione del progetto protocollo informatico è il primo passo per il raggiungimento degli obiettivi di trasparenza previsti in uno dei 10 obiettivi di legislatura.

A tale scopo sono stati avviati dei gruppi di lavoro con alcune amministrazioni per la realizzazione di sistemi integrati di protocollo informatico e di processi amministrativi automatizzati. In questa attività il Project Office offre alle amministrazioni una collaborazione tecnica e acquisisce le informazioni relative ai modelli architetturali dei vari progetti, al loro contesto applicativo, alle problematiche sorte in termini di identificazione degli interlocutori, sicurezza, privacy e quant'altro allo scopo di individuare una casisitica da mettere a disposizione delle amministrazioni che intendano in futuro realizzare progetti analoghi e che pertanto si trovano di fronte a prescindere dal tipo di processo amministrativo da mettere in trasparenza di fronte a problematiche simili.

Rivista "Guida agli enti locali"- Commento di Paolo Subioli relativo al decreto del 14 ottobre 2003 della Presidenza del Consiglio sull'automatizzazione del protocollo informatico. La soluzione per gli uffici in ritardo.

NUMERO SCHEDA: 4189

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: PROTOCOLLO INFORMATICO

FONTE: GUIDA AGLI ENTI LOCALI

AUTORE: Paolo Subioli

NUMERO: 46

DATA: 29/11/2003

PAGINA: 40-42

RIFERIMENTO NORMATIVO: decreto del 14 ottobre 2003 della Presidenza del Consiglio

NATURA ATTO: COMMENTO

SCHEDE COLLEGATE: 3982; 4178;4192

L'autore Paolo Subioli nell'articolo scritto sulla rivista n. 46 "Guida agli enti locali" mette in evidenza quali sono le difficoltà che le amministrazioni pubbliche incontrano nella realizzazione della gestione automatizzata del protocollo informatico e di tutti i procedimenti amministrativi a cominciare dalla complessità tecnica di tale operazione per finire a quella organizzativo-culturale.

Infatti abbandonare l'evidenza concreta e tangibile del documento cartaceo per passare a quello virtuale rappresenta un salto enorme. Così partendo dal presupposto che per molte amministrazioni pubbliche sarà difficile arrivare al 1° gennaio 2004 con un sistema automatizzato funzionante il ministro per l'Innovazione e le tecnologie, Lucio Stanca, ha emanato una nuova direttiva del 20/12/2002 sulle "linee guida in materia di digitalizzazione dell'amministrazione" con la quale concede la possibilità di aver sviluppato un sistema informatico *light* del protocollo e dei procedimenti amministrativi, ossia non sarà necessario aver sviluppato un sistema informatico completo ma sarà sufficiente aver posto le basi per poter successivamente entrare nell'e-government.

Tale direttiva stabilisce le due metodologie con cui applicare il protocollo informatico: 1) il protocollo, automazione delle attività amministrative, formazione e conservazione dei documenti informatici costituiscono un unico e coerente sistema di *governo elettronico;* 2) il protocollo informatico rappresenta il punto di avvio del sistema informatico nel quale l'informazione è di tipo digitale. In questo modo si consente la gestione dei documenti cartacei accanto a quelli informatici purchè tale documento venga acquisito con il protocollo informatico e non con quello tradizionale.

Il commento è consultabile presso il settore Studi e documentazione legislativi.

Rivista "Guida agli enti locali"- Commento di Vincenzo Martorano sul Decreto della presidenza del Consiglio del 14 ottobre 2003 - Partono il 1° gennaio 2004 i sistemi automatizzati degli enti pubblici.

NUMERO SCHEDA: 4178

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: PROTOCOLLO INFORMATICO

FONTE: GUIDA AGLI ENTI LOCALI

AUTORE: Vincenzo Martorano

NUMERO: 46

DATA: 29/11/2003

PAGINA: 38-39

NATURA ATTO: COMMENTO

ORGANO:

SCHEDE COLLEGATE: 3982; 4189; 4192

Il decreto del 14 ottobre 2003 della Presidenza del Consiglio pubblicato nella G.U. del 25 ottobre 2003 fissa per il 1° gennaio 2004 il termine entro il quale tutte le P.A. dovranno provvedere alla realizzazione dei sistemi automatizzati per la gestione del protocollo informatico. L'autore commenta che pur essendo abbastanza gravosa la mole di attività che le amministrazioni sono chiamate a concretizzare, si tratta di una data determinata già da tempo dal testo unico in materia di documentazione amministrativa (art. 50 co. 3 Dpr 445/2000) sulla quale il ministro Stanca ha più volte richiamato l'attenzione ed inoltre con la direttiva del 9 dicembre 2002 ha evidenziato la necessità di predisporre con gradualità una serie di adempimenti preparatori. Per le amministrazioni che non abbiano rispettato la scansione temporale della direttiva prima citata, il documento in esame stabilisce l'obbligo di definire con la massima tempestività un piano d'azione dettagliato che preveda lo svolgimento di determinate attività tra le quali:

- individuazione delle aree organizzative omogenee (AOO);
- adozione del manuale di gestione;
- corsi per la formazione del personale;
- definizione dei progetti volti a fornire all'utenza servizi informativi con canali telematici o mediante l'Urp;
- individuazione dei servizi erogati ai cittadini e alle imprese;
- il miglioramento delle modalità di comunicazione (esterna ed interna).

Il commento è consultabile presso il settore Studi e documentazione legislativi.

Approvate dal Ministro per l'innovazione e le tecnologie le linee guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi in seno alla p.a.

NUMERO SCHEDA: 3982

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: PROTOCOLLO INFORMATICO

FONTE: ITALIA OGGI

DATA: 28/10/2003

NATURA ATTO: LINEE GUIDA

DATA ATTO: 14/10/2003

ORGANO: MINISTERI

SCHEDE COLLEGATE: 4178;4189;4192

Sono state pubblicate sulla Gazzetta Ufficiale n. 249 del 25 ottobre scorso in allegato al decreto 14 ottobre 2003 a firma del Ministro per l'innovazione e le tecnologie, Lucio Stanca, le linee guida per l'adozione in seno alla pubblica amministrazione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi.

Le innovazioni dovranno essere adottate entro tempi strettissimi, posto che il prossimo 1° gennaio 2004 costituisce il termine previsto dalle direttrici ministeriali per rendere operative le novità: entro la suddetta data la p.a. dovrà effettuare la registrazione dei dati e dei documenti esclusivamente mediante protocollo informatico. I registri cartacei saranno pertanto sostituiti da archivi informatici, peraltro già previsti dal T.U. in materia di documentazione amministrativa (dpr 445/2000).

Appositi piani dovranno inoltre essere elaborati dalla p.a. al fine di assicurare la sicurezza dei documenti nonché le modalità di produzione e conservazione delle registrazioni.

La rivoluzione riguarderà anche i procedimenti amministrativi, che dovranno essere gestiti attraverso procedure informatiche, le quali rimpiazzeranno gradualmente il trattamento manuale degli stessi.

Di tali innovazioni gioveranno anche cittadini e imprese, che saranno in grado di conoscere in tempo reale e on-line lo stato delle loro pratiche pendenti, sfruttando le caratteristiche della carta d'identità elettronica e della carta nazionale dei servizi. Inizialmente, in attesa della diffusione di detti strumenti, l'accesso al sistema informatico della p.a. sarà possibile grazie al ricorso alla firma digitale e ai certificati di autenticazione.

Si riporta il testo del decreto.

D.M. 14 ottobre 2003

Approvazione delle linee-guida per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi.

LINEE GUIDA
Per l'adozione del protocollo informatico e per il trattamento informatico dei procedimenti amministrativi
1. INTRODUZIONE E NORMATIVA DI RIFERIMENTO
Con la *Dir.Min. 9 dicembre 2002* del Ministro per l'innovazione e le tecnologie sono stati definiti gli indirizzi per l'adozione delle norme in materia di protocollo informatico e di trattamento elettronico dei procedimenti amministrativi.
Il protocollo informatico e, più in generale, la gestione elettronica dei flussi documentali hanno la finalità di migliorare l'efficienza interna degli uffici attraverso l'eliminazione dei registri cartacei, la riduzione degli uffici di protocollo e la razionalizzazione dei flussi documentali. L'adozione di tali sistemi migliorerà inoltre la trasparenza dell'azione amministrativa attraverso strumenti che facilitano l'accesso allo stato dei procedimenti ed ai relativi documenti da parte di cittadini, imprese ed altre amministrazioni.
Le Pubbliche Amministrazioni dal 1° gennaio 2004, ai sensi dell'art. 50, comma 3, del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*, dovranno, quindi, attenersi ai princìpi e alle norme di seguito indicati:
a) adozione del protocollo informatico per la registrazione dei dati e documenti delle Amministrazioni (art. 50 e ss. del *D.P.R. n. 445 del 2000; decreto del Presidente del Consiglio dei ministri 31 ottobre 2000*, pubblicato sulla Gazzetta Ufficiale 21 novembre 2000, n. 272);
b) trattamento dei procedimenti amministrativi gestito completamente in modo informatico (*legge 7 agosto 1990, n. 241*; *D.P.R. n. 445 del 2000; decreto legislativo 23 gennaio 2002, n. 10*);
c) formazione e conservazione dei documenti informatici (deliberazione Aipa n. 51/2000, pubblicata sulla Gazzetta Ufficiale 14 dicembre 2000, n. 291; deliberazione Aipa n. 42/2001, pubblicata sulla Gazzetta Ufficiale 21 dicembre 2001, n. 296);
d) sottoscrizione elettronica dei documenti informatici (*D.Lgs. n. 10 del 2002; decreto del Presidente del Consiglio dei ministri 8 febbraio 1999; decreto del Presidente della Repubblica 7 aprile 2003, n. 137* - «Regolamento di attuazione della direttiva Comunitaria 93/1999» - su firma elettronica);
e) gestione informatica del sistema documentale e dei flussi documentali (deliberazione Aipa n. 51/2000; deliberazione Aipa n. 42/2001; *D.P.R. n. 445 del 2000*;)
f) accessi telematici ai dati, ai documenti, ai sistemi, alle banche dati (*D.P.R. n. 445 del 2000*, artt. 58, 59 e 60);
g) sicurezza dei dati, dei documenti, delle tecnologie (*decreto legislativo 30 giugno 2003, n. 196*; deliberazione Aipa n. 51/2000, art. 10; *D.P.C.M. 31 ottobre 2000*, art. 7);
h) *Dir.Min. 13 dicembre 2001* direttiva sulla formazione del Ministro per la funzione pubblica, pubblicata su Gazzetta Ufficiale 31 gennaio 2002, n. 26;
i) disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (*legge 27 dicembre 2002, n. 289*, art. 26).
Si tratta di un quadro unitario nell'àmbito del quale il protocollo informatico può essere adottato secondo due tipi di approccio, il primo completo ed il secondo caratterizzato da una gradualità nella realizzazione:
1) nel primo caso, protocollo, automazione della gestione e dell'iter delle attività, formazione e conservazione dei documenti informatici costituiscono un unico sistema di «governo elettronico»;
2) nel secondo caso, il protocollo informatico si pone come il punto di avvio di un sistema amministrativo informatico nel quale l'informazione utilizzata è solo di tipo «digitale», valida in quanto tale, e l'informazione su supporti documentali cartacei viene «trasformata» in digitale.
Ogni Amministrazione, in base alla propria situazione organizzativa e tecnologica, ferma restando la scadenza del 1° gennaio 2004, dovrà valutare la possibilità di adottare l'uno o l'altro approccio, partendo eventualmente da quello minimale per poi evolvere gradualmente verso un sistema gestionale completamente automatizzato.
In tutti i casi, il livello minimale deve essere finalizzato a creare non solo un sistema di protocollo in linea con la normativa ma anche un sistema documentale che si caratterizza per essere un sistema digitale, con la relativa eliminazione dei documenti cartacei una volta trasformati in digitale.
1.1 Scopo delle linee guida e obiettivi strategici
Lo scopo del presente documento è quello di contribuire a creare, fornendo un quadro unitario ed aggiornato, le condizioni organizzative, funzionali e tecnologiche per la progettazione, la realizzazione, lo sviluppo e la revisione dei sistemi informativi automatizzati al fine di avviare, entro l'anno 2003 e quindi dal 1° gennaio 2004, il protocollo informatico e gestire i procedimenti amministrativi in modo elettronico. Il documento è rivolto a tutte le Amministrazioni pubbliche e si prefigge di fornire alle

stesse un supporto nell'interpretazione e attuazione delle leggi, al fine di contribuire a promuovere una revisione sostanziale dei procedimenti amministrativi, cogliendo così lo spirito della norma che ha inteso creare i presupposti di una semplificazione dei procedimenti amministrativi ed una maggior trasparenza dei processi verso il cittadino e l'impresa.
Nel documento vengono esaminati gli adempimenti delle Amministrazioni, le funzionalità minime, la gestione documentale e la gestione dei flussi lavorativi, dando risalto alle attività che l'Amministrazione deve svolgere per ciascuna delle suddette fasi.
Le linee guida in particolare riguardano:
1. gli adempimenti ai quali sono tenute le Amministrazioni:
• assicurare le funzionalità minime di protocollo;
• procedere all'archiviazione della documentazione sulla base del criterio per cui tutta la documentazione in ingresso diventa «digitale» secondo la normativa tecnica;
• pianificare le attività al fine di realizzare un sistema di base protocollo-archiviazione che permetta di avviare il sistema documentale informatico sostitutivo di quello cartaceo;
• accedere al protocollo-archivio informatico «solo» tramite una rete interna all'amministrazione anche al fine di eliminare la duplicazione di documenti e fascicoli cartacei, con significative economie gestionali sia interne sia per l'utenza;
• pianificare le attività finalizzate alla gestione informatica dei procedimenti amministrativi al fine di sostituire, anche in modo graduale, il trattamento manuale degli stessi procedimenti;
2. la funzionalità minima da assicurare per l'avvio del protocollo informatico;
3. i requisiti dei sistemi documentali e procedimentali che costituiscono un vincolo progettuale e realizzativo ma anche una opportunità per avviare modalità omogenee di operatività;
4. aspetti tecnologici.
Le presenti linee guida forniscono un quadro di riferimento generale di carattere normativo e, unitamente ai precedenti documenti emessi dall'Aipa, «Studio di prefattibilità sul Sistema di gestione dei flussi di documenti (Sistema GEDOC)», «Linee guida alla realizzazione dei sistemi di protocollo informatico e gestione dei flussi documentali nelle pubbliche amministrazioni» (GEDOC2), «Interoperabilità dei sistemi di protocollo informatico in ambiente distribuito», e a quelli in via di elaborazione, intende offrire un insieme organico di strumenti di supporto per le Amministrazioni.
1.2 Centro di Competenza
Con la *Dir.Min. 9 dicembre 2002* pubblicata sulla Gazzetta Ufficiale del 5 marzo 2003, n. 53, il Ministro per l'innovazione e le tecnologie, ha creato presso il Centro Tecnico per la R.U.P.A. un Centro di competenza per il Progetto Protocollo informatico e trasparenza amministrativa quale unico punto di riferimento, che svolge, in continuità con le attività già svolte dall'Aipa, funzioni di indirizzo e coordinamento e che promuove iniziative di affiancamento per garantire l'attuazione della direttiva, in particolare attraverso:
• le informazioni, le esperienze e i servizi messi a disposizione sul sito web sulla gestione elettronica dei documenti (http://protocollo.gov.it), le cui finalità sono la condivisione delle migliori pratiche e la sussidiarietà;
• la collaborazione fornita dal Centro dì competenza che può essere contattato al seguente indirizzo di posta elettronica: cc@protocollo.gov.it; .
• incontri periodici con i referenti delle Amministrazioni allo scopo di verificare lo stato di avanzamento delle attività.
Tra i suoi compiti in particolare si segnalano:
• azioni di sensibilizzazione e comunicazione;
• rilevazione periodica dello stato di attuazione dei progetti;
• supporto alle amministrazioni, secondo un princìpio di sussidiarietà, attraverso l'erogazione di un servizio di gestione del protocollo informatico e dei flussi documentali in modalità ASP.
2. ADEMPIMENTI DELLE AMMINISTRAZIONI.
Le Pubbliche Amministrazioni, al fine di adottare entro il 1 ° gennaio 2004 il protocollo informatico e gestire i procedimenti amministrativi in modo elettronico, sono tenute ai seguenti interventi:
a) provvedere ad introdurre, nei piani di sviluppo dei sistemi informativi automatizzati, progetti per la realizzazione di sistemi di protocollo informatico (art. 50, comma 1, del *D.P.R. n. 445 del 2000)*.
b) predisporre appositi progetti esecutivi per la sostituzione dei registri di protocollo cartacei con sistemi informatici (art. 50, comma 2, del *D.P.R. n. 445 del 2000*;)
c) realizzare o revisionare i propri sistemi informativi (art. 50, comma 3, del *D.P.R. n. 445 del 2000*;)

I progetti dovranno essere pianificati in termini organizzativi, funzionali, tecnologici e finanziari, nel rispetto della data del 1° gennaio 2004. Il progetto esecutivo ha lo scopò di definire attività, tempi e costo-benefici per l'operazione di sostituzione anche ai sensi della deliberazione Aipa n. 42/2001.
Il sistema informativo viene considerato come un insieme integrato di dati, funzioni e tecnologie finalizzato non solo alla registrazione di dati e documenti in ingresso ed in uscita, ma anche all'automazione del sistema procedimentale e documentale (protocollo, iter delle attività, atti e provvedimenti, documenti e modulistica, accessi telematici).
Le Amministrazioni hanno l'obbligo di operare attraverso un piano di automazione adottato o da adottare, con riferimento al proprio ordinamento, per attuare quanto stabilito dal *D.P.R. n. 445 del 2000* e secondo le norme tecniche vigenti (art. 51, comma 1, del *D.P.R. n. 445 del 2000)*.
Le stesse devono rivedere i sistemi informativi al fine di realizzare una automazione totale delle fasi di produzione, gestione, diffusione ed utilizzazione dei propri dati, documenti, procedimenti ed atti (art. 51, comma 2, del *D.P.R. n. 445 del 2000)*.
Gli interventi dovranno quindi comprendere una necessaria e preliminare azione di razionalizzazione e semplificazione delle attività, dei procedimenti, della documentazione e della modulistica (art. 3, comma 3, della deliberazione Aipa 51/2000).
Allo scopo di fornire un promemoria e un valido supporto per una corretta scanzione temporale delle attività sopra riportate, la direttiva del Ministro per l'innovazione e le tecnologie ha previsto fasi intermedie fino alla scadenza del 1° gennaio 2004. A questo fine le Amministrazioni che non abbiano ancora provveduto devono definire, con la massima tempestività, un piano d'azione dettagliato - il quale preveda lo svolgimento delle attività sotto elencate tenendo conto della citata scadenza per l'adozione del sistema di protocollo informatico - e comunicare tale piano al Centro Tecnico per la R.U.P.A., tramite il sito web http://protocollo.gov.it.
Più in dettaglio è necessario:
1. individuare le Aree organizzative omogenee (AOO) e i relativi uffici di riferimento ai sensi dell'articolo 50, comma 4, del *D.P.R. n. 445 del 2000*
2. comunicare al Centro Tecnico la casella ufficiale di posta elettronica per l'iscrizione delle AOO nell'indice delle P.A.;
3. comunicare al Centro Tecnico, per ogni AOO istituita, il nominativo del responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61, comma 2, del *D.P.R. n. 445 del 2000*;
4. adottare, per ogni AOO istituita, il manuale di gestione come previsto dalle regole tecniche di cui all'articolo 5 del *D.P.C.M. 31 ottobre 2000*;
5. pubblicare e rendere accessibile tramite internet il manuale di gestione che descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni necessarie per il corretto funzionamento del servizio, per la tenuta del protocollo informatico (cfr. par. 2.1.1);
6. predisporre un progetto operativo per la progressiva messa in opera di sistemi di protocollo informatico integrati con la posta elettronica certificata e la firma elettronica ai sensi dell'articolo 10, comma 3, del *D.P.R. n. 445 del 2000* nel rispetto dei princìpi di interoperabilità di cui alla *circolare 7 maggio 2001* Aipa;
7. predisporre correlate attività di formazione, d'intesa con il Dipartimento della funzione pubblica ai sensi della *Dir.Min. 13 dicembre 2001* Direttiva sulla formazione del Ministro per la funzione pubblica;
8. fornire informazioni al Centro Tecnico per la R.U.P.A. sull'avanzamento dei progetti, al fine di permettere delle rilevazioni periodiche sullo stato di attuazione della normativa.
Inoltre, le Amministrazioni, per l'attuazione della trasparenza dell'attività amministrativa, devono svolgere, ove non vi abbiano provveduto entro la prevista scadenza, le seguenti azioni:
1. comunicare al Centro Tecnico il nome di un referente, al fine di definire le attività di interesse comune e concordarne i relativi tempi di realizzazione;
2. individuare i servizi di propria competenza erogati ai cittadini e alle imprese sia con modalità tradizionali sia in rete;
3. pianificare, secondo criteri di priorità, l'attuazione della trasparenza dell'azione amministrativa come definita in precedenza, tramite la predisposizione di progetti orientati a fornire ai cittadini e alle imprese servizi informativi con canali telematici diretti o attraverso intermediazione dell'Ufficio relazioni con il pubblico;
4. migliorare la comunicazione tra gli uffici e gli URP al fine di migliorare la comunicazione esterna e l'esercizio del diritto di accesso;
5. compilare, per ogni progetto una scheda informativa, secondo lo schema riportato in allegato alla direttiva, da inviare al Centro tecnico.

Le Amministrazioni, poi, con riferimento al proprio ordinamento, devono:
a) pianificare le attività per la eliminazione dei diversi tipi di protocollo attivati, di cui all'articolo 3, comma 1, lettera *d*) del *D.P.C.M. 31 ottobre 2000*;
b) accreditare l'Amministrazione presso l'IPA - Indice della Pubblica Amministrazione (articolo 12 del *D.P.C.M. 31 ottobre 2000* recante Regole tecniche per il protocollo informatico); informazioni in proposito si trovano sul sito http://indicepa.gov.it
La direttiva è indirizzata a tutte le Amministrazioni centrali dello Stato e agli enti pubblici sottoposti alla vigilanza ministeriale. Per le regioni e gli enti locali territoriali la stessa costituisce contributo alle determinazioni in materia, nel rispetto della propria autonomia amministrativa. La direttiva può rappresentare uno schema di riferimento anche per le altre Amministrazioni pubbliche di cui all'articolo 1, comma 2, del *decreto legislativo 30 marzo 2001, n. 165*.
2.1 Analisi ed individuazione delle Aree organizzative omogenee
Analisi organizzativa
Preliminarmente si dovrebbe procedere all'analisi dei processi per la loro semplificazione, articolandola per fasi:
fase 1: definizione del campo di applicazione dell'intervento organizzativo
passo 1 - identificare l'àmbito e i livelli di intervento;
passo 2 - delineare il contesto;
passo 3 - fissare gli obiettivi;
fase 2: diagnosi delle criticità e delle priorità;
passo 4 - ricostruire la mappa dei processi reali;
passo 5 - definire le metriche della prestazione complessiva di processo;
passo 6 - misurare la distanza fra obiettivi e situazione attuale;
fase 3: riprogettazione dei processi;
passo 7 - disegnare le alternative di riprogettazione;
passo 8 - progettare il sistema di monitoraggio e controllo;
passo 9 - preparare la gestione del cambiamento organizzativo;
passo 10 - sperimentare e correggere le ipotesi di riprogettazione.
Definizione delle Aree organizzative omogenee
Attraverso la individuazione e la definizione delle Aree organizzative omogenee (AOO) si rideterminano gli àmbiti dei nuovi sistemi di protocollo informatico. Questa individuazione consente di arrivare ad una diminuzione e semplificazione dell'insieme dei sistemi di protocollo oggi esistenti. Il fenomeno della frammentazione dei registri di protocollo è una delle maggiori cause di inefficienze nella gestione dei documenti delle Pubbliche Amministrazioni. Tra le conseguenze negative derivanti da tale frammentazione va certamente citata la ripetuta protocollazione del documento (con annesse le operazione di registrazione di dati ridondanti) ad ogni passaggio anche tra strutture interne alla stessa Amministrazione, oltre alle notevoli difficoltà di reperimento del documento protocollato tali da rendere, paradossalmente, l'individuazione della collocazione fisica del documento un problema secondario rispetto all'individuazione del registro di protocollo in cui esso è stato registrato.
Una AOO può essere definita come un insieme di unità organizzative dell'Amministrazione che usufruiscono, in modo omogeneo e coordinato, degli stessi servizi per la gestione dei flussi documentali. Una unità organizzativa associata ad una AOO è un utente dei servizi messi a disposizione dalla AOO stessa. Una AOO offre, in particolare, il servizio di protocollo dei documenti in entrata ed in uscita che avviene utilizzando una unica sequenza numerica, rinnovata ad ogni anno solare, propria all'area stessa (art. 61 *D.P.R. n. 445 del 2000)*. Per ulteriori approfondimenti si può fare riferimento al documento «Linee guida alla realizzazione dei sistemi di protocollo informatico e gestione dei flussi documentali nelle pubbliche amministrazioni» (GEDOC2).
Le Amministrazioni, al termine di questo processo di analisi, devono comunicare al Centro Tecnico per la R.U.P.A. la casella ufficiale di posta elettronica per l'iscrizione delle AOO nell'Indice della Pubblica Amministrazione.
2.2 Il manuale di gestione
Il manuale di gestione, di cui all'articolo 5 del *D.P.C.M. 31 ottobre 2000*, descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico.
Il responsabile del servizio di cui all'articolo 61 del *D.P.R. n. 445 del 2000* ha il compito di predisporre lo schema del manuale di gestione.
L'articolo 5 del predetto decreto è strutturato come un «indice» del manuale e ciò facilita la redazione dello stesso; sono citati in particolare i seguenti punti:

a) la pianificazione, le modalità e le misure di cui all'articolo 3, comma 1, lettera *d*);
b) il piano di sicurezza dei documenti informatici di cui all'articolo 4, comma 4;
c) le modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'area organizzativa omogenea;
d) la descrizione del flusso di lavorazione dei documenti ricevuti, spediti o interni, incluse le regole di registrazione per i documenti pervenuti secondo particolari modalità di trasmissione, tra i quali, in particolare, documenti informatici di fatto pervenuti per canali diversi da quelli previsti dall'articolo 15 del presente decreto, nonché fax, raccomandata, assicurata;
e) l'indicazione delle regole di smistamento ed assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione e/o verso altre amministrazioni;
f) l'indicazione delle unità organizzative responsabili delle attività di registrazione di protocollo, di organizzazione e tenuta dei documenti all'interno dell'area organizzativa omogenea;
g) l'elenco dei documenti esclusi dalla registrazione di protocollo;
h) l'elenco dei documenti soggetti a registrazione particolare e le relative modalità di trattamento;
i) il sistema di classificazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, anche con riferimento all'uso di supporti sostitutivi;
l) le modalità di produzione e di conservazione delle registrazioni di protocollo informatico ed in particolare l'indicazione delle soluzioni tecnologiche ed organizzative adottate per garantire la non modificabilità della registrazione di protocollo, la contemporaneità della stessa con l'operazione di segnatura, nonché le modalità di registrazione delle informazioni annullate o modificate nell'àmbito di ogni sessione di attività di registrazione;
m) la descrizione funzionale ed operativa del sistema di protocollo informatico con particolare riferimento alle modalità di utilizzo;
n) i criteri e le modalità per il rilascio delle abilitazioni di accesso interno ed esterno alle informazioni documentali;
o) le modalità di utilizzo del registro di emergenza, inclusa la funzione di recupero dei dati protocollati manualmente.
La corretta ed efficace attuazione delle norme in materia di protocollo e di sistema documentale informatico è strettamente correlata alla redazione del manuale.
Per sua natura e struttura il manuale comprende analisi, decisioni, piani, iter delle attività, classificazioni, ecc., definiti in relazione alle specificità organizzative, funzionali, strutturali e di servizio dell'Amministrazione di riferimento.
È compito dei dirigenti e dei funzionari partecipare alla redazione del manuale, per quanto riguarda le informazioni relative all'unità organizzativa di competenza, anche in relazione alla pubblicità del manuale stesso.
Il manuale di gestione deve essere reso pubblico ed accessibile sia tramite internet (possibilmente sul sito del protocollo), sia attraverso supporti informatici o cartacei; deve essere redatto in modo chiaro, completo, e deve essere periodicamente aggiornato.
Il manuale è quindi l'insieme delle regole certificate dall'Amministrazione per un corretto ed efficace funzionamento del sistema di protocollo, dei procedimenti amministrativi informatici e del sistema documentale.
Lo schema del manuale è «comune» (di tipo «standard») ma la redazione non può che essere effettuata su «misura» dell'Amministrazione di riferimento, in quanto sono compresi interventi di tipo organizzativo, procedurale ed informatico specifici dell'ente in questione, non «trasferibili», in modo asettico e generalizzato, a tutti gli organismi pubblici.
Una bozza di schema del manuale può essere consultata sul sito http://protocollo.gov.it. Alcune indicazioni utili per la redazione del manuale sono ricavabili anche da alcuni esempi già realizzati pubblicati sul sito http://protocollo.gov.it.
Nei paragrafi che seguono sono riportati brevi suggerimenti sulle attività previste nell'àmbito della redazione del manuale.
2.2.1 Adozione di un protocollo unico.
Gli obiettivi da realizzare sono i seguenti:
pianificazione, modalità e misure di cui all'articolo 3, comma 1, lettera *d*) del *D.P.C.M. 31 ottobre 2000:*
eliminazione dei diversi protocolli di settore, di reparto, multipli per l'adozione di un unico protocollo (art. 5, comma 2, lettera *a*).
Le attività che discendono dall'applicazione della norma sono le seguenti:

• censimento dei diversi protocolli;
• analisi dei livelli di automazione;
• interventi organizzativi, procedurali e tecnici da effettuare per adottare il protocollo informatico;
• tempi di sostituzione;
• costi.

2.2.2 Piano di sicurezza dei documenti informatici

Il responsabile del servizio di cui all'articolo 61 del *D.P.R. n. 445 del 2000* ha il compito di predisporre il piano di sicurezza secondo quanto previsto dall'articolo 5, comma 2, lettera *b*), del *D.P.C.M. 31 ottobre 2000*.

Le attività che discendono dall'applicazione della norma sono le seguenti:
• analisi dei rischi in relazione alla tipologia dei documenti;
• analisi dei rischi in relazione alla tipologia dei dati personali (*D.Lgs. n. 196 del 2003*;)
• misure di sicurezza da adottare di tipo organizzativo, procedurale e tecnico;
• formazione dei dipendenti;
• monitoraggio periodico del piano di sicurezza.

In particolare, il manuale dovrà fare riferimento ai requisiti di sicurezza di cui al punto 2.2.11.

2.2.3 Scambio di documenti.

Con riferimento alle modalità di utilizzo di strumenti informatici per lo scambio di documenti all'interno ed all'esterno dell'area organizzativa omogenea, di cui all'articolo 5, comma 2, lettera *c*), del *D.P.C.M. 31 ottobre 2000*, le attività che discendono dall'applicazione della norma sono le seguenti:
• rilevazione dei flussi documentali all'interno dell'ente (o delle AOO) e verso altri enti (o altre AOO);
• mappatura dei flussi;
• modalità e tecnologie per lo scambio dei documenti.

La rilevazione dei flussi documentali è facilitata se viene effettuata nell'àmbito di un censimento più ampio che comprenda anche le attività, le procedure, i procedimenti, la modulistica utilizzata (v. il punto successivo).

2.2.4 Descrizione del flusso di lavorazione dei documenti

La descrizione nel flusso documentale dei documenti ricevuti, spediti o interni di cui all'articolo 5, comma 2, lettera *d*), del *D.P.C.M. 31 ottobre 2000*, costituisce l'aspetto fondamentale di tutto il processo di automazione del sistema documentale e procedimentale in quanto solo la conoscenza completa dell'iter delle attività permette di realizzare anche un processo di automazione in linea con i princìpi di trasparenza, efficienza, efficacia ed economicità.

Le attività che discendono dall'applicazione della norma sono le seguenti:
• censimento di tutte le attività dell'ente (o dell'area organizzativa omogenea) al fine di descrivere la lavorazione dei documenti; il censimento dovrebbe riguardare i dati di base di ciascuna attività (denominazione, allocazione, durata, flusso procedurale, modulistica, norme di riferimento, fasi, risorse umane impegnate, pareri, ecc.);
• analisi del risultato del censimento;
• interventi di razionalizzazione delle singole attività;
• piano di automazione delle attività;
• regole di registrazione dei documenti.

2.2.5 Regole di smistamento ed assegnazione dei documenti ricevuti.

Le attività che discendono dall'applicazione della norma di cui all'articolo 5, comma 2, lettera *e*) del *D.P.C.M. 31 ottobre 2000*, concernenti le regole di smistamento ed assegnazione dei documenti ricevuti, sono le seguenti:
• a seguito della registrazione dei documenti in entrata è necessario stabilire le regole per lo smistamento, l'assegnazione e la lavorazione degli stessi da parte dei responsabili dei procedimenti e nell'àmbito delle aree organizzative omogenee;
• se si considera che i documenti sono per definizione «informatici» (o resi tali, se ricevuti come cartacei) allora sarà necessario definire con chiarezza e completezza le modalità di smistamento ed assegnazione di tipo elettronico, anche in considerazione di quanto stabilisce la *legge n. 241 del 1990* ed il relativo regolamento.

2.2.6 Unità organizzative responsabili delle attività di registrazione e della documentazione

Le attività che discendono dall'applicazione della norma di cui articolo 5, comma 2, lettera *f*), del *D.P.C.M. 31 ottobre 2000*, concernente le unità organizzative responsabili delle attività di registrazione e della documentazione sono le seguenti:

• nell'àmbito dell'area organizzativa omogenea, e con riferimento al sistema organizzativo dell'Ente, è necessario indicare le unità organizzative responsabili delle attività di registrazione e di organizzazione e tenuta della documentazione;
• nel manuale sarà necessario quindi definire le funzioni specifiche di tali unità organizzative ed il profilo dei dipendenti che operano in tali unità.

2.2.7 Documenti esclusi dalla registrazione di protocollo

Le attività che discendono dall'applicazione della norma di cui all'articolo 5, comma 2, lettere *G* e *H* del *D.P.C.M. 31 ottobre 2000*, concernenti i documenti esclusi dalla registrazione di protocollo, sono le seguenti:
• riportare nel manuale l'elenco dei documenti esclusi dalla registrazione di protocollo ai sensi dell'articolo 53, comma 5, del *D.P.R. n. 445 del 2000*.
• riportare l'elenco dei documenti soggetti a registrazione particolare e le relative modalità di trattamento.

Tali documenti vanno individuati dall'Amministrazione e possono essere registrati attraverso applicazioni diverse dal sistema di protocollo informatico.

2.2.8 Il sistema di classificazione dei documenti

Il sistema di classificazione è lo strumento che permette di organizzare tutti i documenti secondo un ordinamento logico, con riferimento alle funzioni e alle attività dell'Amministrazione interessata.
Le attività che discendono dall'applicazione della norma di cui all'articolo 5, comma 2, lettera *i*), del *D.P.C.M. 31 ottobre 2000*, sono le seguenti:
• il sistema di classificazione dei documenti dovrà essere definito in ragione dell'ordinamento, dell'organizzazione e dei servizi della stessa Amministrazione.

In particolare, la classificazione dovrà basarsi sui seguenti princìpi:
• omogeneità tematica che caratterizza la stessa AOO (omogeneità funzionale) e che da questa viene prodotta a sua volta;
• autonomia dei documenti rispetto alla struttura organizzativa di riferimento che nel tempo può anche mutare di denominazione, articolazione e funzioni;
• reperibilità del documento, in primo luogo, rispetto all'argomento ed ai contenuti e, in secondo luogo, rispetto alla struttura organizzativa di riferimento.

Il sistema di classificazione può seguire le regole generali definite dalla classificazione decimale.
I sistemi di ricerca elettronica dovranno tenere conto del sistema di classificazione.
Nel manuale dovranno essere indicate inoltre:
• le modalità di aggiornamento del sistema;
• tempi, criteri e regole di selezione e di conservazione;
• l'uso di supporti sostitutivi.

Ulteriori suggerimenti possono essere trovati nel documento «Linee guida alla realizzazione dei sistemi di protocollo informatico e gestione dei flussi documentali nelle pubbliche amministrazioni (GEDOC2)», reperibile nel sito web http://protocollo.gov.it.

2.2.9 Modalità di produzione e conservazione delle registrazioni

Le attività che discendono dall'applicazione della norma dì cui all'art. 5, comma 2, lettera *l*), del *D.P.C.M. 31 ottobre 2000*, concernenti le modalità di produzione e conservazione delle registrazioni, consistono nel riportare nel manuale:
• le modalità di produzione e di conservazione delle registrazioni di protocollo informatico;
• l'indicazione, delle soluzioni tecnologiche ed organizzative adottate per garantire la non modificabilità della registrazione di protocollo;
• la contemporaneità della registrazione con l'operazione di segnatura;
• le modalità di registrazione delle informazioni annullate o modificate nell'àmbito di ogni sessione di attività di registrazione.

In particolare, per quanto riguarda le informazioni annullate il manuale dovrà fare riferimento a quanto stabilito nell'articolo 8 del *D.P.C.M. 31 ottobre 2000* (Annullamento delle informazioni registrate in forma non modificabile).

2.2.10 Funzionalità del sistema di protocollo informatico

Le attività che discendono dall'applicazione della norma di cui all'articolo 5, comma 2, lettera *m*), del *D.P.C.M. 31 ottobre 2000*, concernenti la funzionalità del sistema di protocollo informatico sono le seguenti:
• il manuale deve contenere la descrizione funzionale ed operativa del sistema di protocollo informatico con particolare riferimento alle modalità d'uso;

• la descrizione dovrà essere effettuata con lo scopo di indicare con chiarezza e completezza l'utilizzabilità del sistema da parte di tutti coloro che sono abilitati ad operare nel sistema documentale e procedimentale dell'amministrazione. Il grado di chiarezza e completezza è strettamente correlato al grado di chiarezza e completezza di tutte le regole descritte nel manuale.

2.2.11 Abilitazioni per l'accesso al sistema documentale

Le attività che discendono dall'applicazione della norma di cui all'articolo 5, comma 2, lettera *n*), del *D.P.C.M. 31 ottobre 2000*, consistono nell'individuazione, con riferimento al tipo di accesso, dei criteri e delle modalità per il rilascio delle abilitazioni all'interno e all'esterno dell'amministrazione.

Il manuale deve pertanto contenere la descrizione delle politiche di accesso ai documenti che l'Amministrazione intende adottare:

• definendo, relativamente all'accesso ai documenti per gli utenti interni, i criteri di visibilità sulla base di ruoli e funzioni svolte dai dipendenti;

• classificando, per quanto riguarda l'acceso da parte di utenti esterni (cittadini, imprese, altre amministrazioni), le modalità relative in due tipologie:

- dirette se l'amministrazione ha previsto un canale di comunicazione con l'esterno in maniera automatizzata (es. via internet);

- indirette nel caso in cui l'amministrazione permetta l'accesso ai documenti tramite una struttura di contatto con l'esterno (es. Ufficio Relazioni con il Pubblico, Call center ecc.).

2.2.12 Registro di emergenza

Le attività che discendono dall'applicazione della norma di cui all'articolo 5, comma 2, lettera *o*), del *D.P.C.M. 31 ottobre 2000*, concernente il registro di emergenza, sono le seguenti:

• riportare sul registro di emergenza la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema (art. 63, comma 1 del *D.P.R. n. 445 del 2000*;)

• il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi deve dare l'autorizzazione ad operare in modo manuale (art. 63, comma 1 del *D.P.R. n. 445 del 2000*;)

• riportare sul registro di emergenza le autorizzazioni all'uso di procedure manuali per periodi successivi alle 24 ore ed il numero totale di operazioni registrate manualmente.

3. PIANO OPERATIVO.

Il piano di attuazione prevede un censimento preliminare dei diversi protocolli esistenti, l'analisi dei livelli di automazione, ma soprattutto gli interventi organizzativi, procedurali e tecnici da effettuare per adottare il protocollo informatico con i tempi di sostituzione e i costi derivanti. Uno dei primi obiettivi che ciascuna Amministrazione si deve dare nel definire un progetto di informatizzazione dei flussi documentali, è quello di individuare il proprio «livello realizzativo», corrispondente alle funzionalità che essa stessa vuole realizzare.

Le Amministrazioni definiscono quindi un piano d'azione dettagliato che preveda lo svolgimento delle attività elencate nel paragrafo 2, tenendo conto della citata scadenza del 1° gennaio 2004, prevista dal *D.P.R. n. 445 del 2000* per l'adozione del sistema di protocollo informatico. Tale piano d'azione deve essere inviato al Centro Tecnico per la R.U.P.A. attraverso il sito httt://protocollo.gov.it.

3.1 Organizzazione del personale e formazione

Nella fase di analisi organizzativa, gli elementi principali da tenere in considerazione sono:

• la formazione culturale del personale;

• il piano di formazione obbligatorio ai sensi della *Dir.Min. 13 dicembre 2001* del Ministero della funzione pubblica;

• il dimensionamento degli organici tenendo presente la diversa organizzazione derivante dall'introduzione di un protocollo informatico (scadenze e tempi di inserimento dei documenti da protocollare);

• l'organizzazione di un servizio di *help desk* per gli utilizzatori del protocollo;

• la definizione dei profili professionali;

• l'assegnazione di incarichi di coordinamento;

• l'individuazione di referenti e capi progetto a seconda delle dimensioni dell'Amministrazione e quindi della tipologia di progetto previsto.

All'analisi organizzativa si deve affiancare un progetto di formazione e comunicazione che deve essere di esempio e di impulso per l'intera Amministrazione. Deve essere in particolare prevista la realizzazione di un programma di formazione differenziato a seconda dei destinatari e articolato in moduli sia teorici che operativi per avviare e monitorare il processo di evoluzione delle competenze manageriali e professionali al fine di renderle più rispondenti e coerenti con le nuove esigenze. Il programma di formazione dovrà essere integrato da interventi di comunicazione, opportunamente pianificati, volti a

migliorare il coinvolgimento e la sensibilizzazione del personale, promuovendone l'adesione agli obiettivi da raggiungere.

3.2 Servizi verso cittadini e imprese

Lo sviluppo della Società dell'Informazione è una delle priorità del Governo: in questo contesto la prestazione di servizi on-line assume una particolare rilevanza.

La finalità da perseguire è quella di permettere a cittadini e imprese di conoscere in tempi reali le informazioni relative allo stato delle attività amministrative di proprio interesse, migliorando di conseguenza l'efficienza, l'efficacia e l'immagine della Pubblica Amministrazione.

Il *D.P.R. n. 445 del 2000*, con riferimento ai princìpi stabiliti dalla *legge n. 241 del 1990*, ha definito tre tipi di accesso ai dati, documenti ed informazioni del sistema informatico:

a) l'accesso al sistema da parte degli utenti appartenenti all'Amministrazione (art. 58 del *D.P.R. n. 445 del 2000*;)

b) l'accesso esterno al sistema da parte dei soggetti che esercitano il diritto di accesso ai documenti amministrativi (art. 59 del *D.P.R. n. 445 del 2000*;)

c) l'accesso al sistema di una pubblica amministrazione da parte di altre amministrazioni (art. 60 del *D.P.R. n. 445 del 2000)*.

Per tutti i tipi di accesso, anche ai sensi della *D.Lgs. n. 196 del 2003*, le Amministrazioni dovranno definire le abilitazioni necessarie e le diverse modalità di interrogazione, selezione ed estrazione delle informazioni, a seconda del grado di riservatezza delle stesse e della tipologia di utenti, utilizzando firma digitale o certificati di autenticazione.

In seguito, quindi, per l'accesso sicuro ai documenti potranno essere previste diverse modalità di identificazione e accreditamento degli utenti tramite strumenti quali la carta d'identità elettronica o la carta nazionale dei servizi.

4. FUNZIONALITÀ MINIME DEL PROTOCOLLO.

Le Amministrazioni devono garantire almeno la realizzazione del sistema di protocollo secondo i requisiti di operazioni ed informazioni, definite «funzionalità minime», di cui agli articoli 53, 55 e 56 del *D.P.R. n. 445 del 2000*. Le operazioni di registrazione e di segnatura di protocollo indicate rispettivamente all'articolo 53 e all'articolo 55 nonché quelle di classificazione costituiscono attività necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni. In particolare si sottolinea che

a) con riferimento ai requisiti della registrazione, la registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni:

• numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;

• data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;

• mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;

• oggetto del documento, registrato in forma non modificabile;

• data e protocollo del documento ricevuto, se disponibili;

• l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.

b) con riferimento ai requisiti della segnatura, le informazioni minime previste sono:

• il progressivo di protocollo, secondo il formato disciplinato all'articolo 57;

• la data di protocollo;

• l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa individuata ai sensi dell'articolo 50, comma 4.

c) con riferimento alla classificazione dei documenti, vedasi punto precedente 2.2.8.

Il piano di classificazione o titolario di archivio si presenta, generalmente, come uno schema generale di voci logiche, stabilite in modo uniforme, rispondenti ai bisogni funzionali del soggetto produttore e articolate tendenzialmente in modo gerarchico al fine di identificare secondo uno schema logico che va dal generale al particolare l'unità archivistica, cioè l'unità di aggregazione di base dei documenti all'interno dell'archivio (ad esempio, il fascicolo, il registro, ecc.) entro cui i documenti sono ordinati secondo le funzioni/attività/affari e/o materie di cui partecipano.

Per garantire le funzionalità minime, sotto il profilo documentale e tecnologico, il sistema di protocollo sarà costituito da risorse informatiche destinate non solo alla registrazione e alla segnatura ma anche alla conservazione della documentazione, secondo la deliberazione Aipa n. 42/2001 al fine di rendere

concreto l'accesso alla documentazione da parte dei dipendenti abilitati sia in modalità locale che remota.
Nei paragrafi seguenti vengono presentati i requisiti normativi applicabili per la realizzazione del nucleo minimo in un sistema di protocollo informatico.
4.1 Requisiti della registrazione di protocollo
La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni secondo l'articolo 53 del *D.P.R. n. 445 del 2000* è effettuata mediante la memorizzazione delle seguenti informazioni:
• numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
• data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
• mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
• data e protocollo del documento ricevuto, se disponibili;
• l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile.
Altri requisiti previsti:
• Il sistema deve consentire la produzione del registro giornaliero di protocollo (art. 53, comma 2, del *D.P.R. n. 445 del 2000*;)
• L'assegnazione delle informazioni nelle operazioni di registrazione di protocollo è effettuata dal sistema in unica soluzione, con esclusione di interventi intermedi, anche indiretti, da parte dell'operatore, garantendo la completezza dell'intera operazione di modifica o registrazione dei dati;
• Per quanto riguarda l'impronta del documento si rinvia a quanto definito dall'articolo 17 del *D.P.C.M. 31 ottobre 2000*.
Tutti i requisiti sopra riportati permettono di costruire un sistema di protocollo a supporto della trasparenza e della certezza del sistema amministrativo.
4.2 Requisiti della segnatura di protocollo
Le informazioni minime previste per la segnatura secondo l'articolo 55 del *D.P.R. n. 445 del 2000* sono:
a) il progressivo di protocollo, secondo il formato di cui all'articolo 57;
b) la data di protocollo;
c) l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa individuata ai sensi dell'articolo 50, comma 4.
Le informazioni da includere nella segnatura sono definite dall'articolo 19 del *D.P.C.M. 31 ottobre 2000*.
L'operazione di segnatura di protocollo va effettuata contemporaneamente all'operazione di registrazione di protocollo.
Per quanto riguarda i requisiti del formato di segnatura si rinvia all'articolo 9 del *D.P.C.M. 31 ottobre 2000*.
Per ciò che concerne la segnatura dei documenti trasmessi si rinvia all'articolo 18 del *D.P.C.M. 31 ottobre 2000*.
4.3 Requisiti di sicurezza del sistema documentale e del sistema di protocollo informatico
Il piano di sicurezza dei documenti informatici è previsto dall'articolo 7 del *D.P.C.M. 31 ottobre 2000* e dall'articolo 10 della deliberazione Aipa n. 51 del 2000, in attuazione dell'articolo 18 del *D.P.R. n. 513 del 1997*, come modificato dall'art. 9, comma 4 del *D.P.R. n. 445 del 2000*.
Il piano di sicurezza deve considerare almeno i seguenti aspetti:
• analisi dei rischi;
• politiche di sicurezza;
• interventi operativi;
• misure di sicurezza per la tutela dei dati personali;
• verifica ed aggiornamento del piano.
In particolare, l'articolo 7 del *D.P.C.M. 31 ottobre 2000* definisce i requisiti minimi di sicurezza dei sistemi di protocollo informatico.
5. GESTIONE DOCUMENTALE E GESTIONE DEI FLUSSI DI LAVORO.
Per Gestione documentale si intende la gestione informatica dei documenti in modalità avanzata.
Si tratta di una soluzione che privilegia ed esalta essenzialmente le potenzialità legate alla gestione informatizzata dei documenti e degli archivi. Essa consiste in realtà in attività assai eterogenee, che variano a seconda del grado di funzionalità da attuare, ma che trovano il loro comune presupposto

fondamentale nella dematerializzazione dei documenti cartacei e quindi della disponibilità degli stessi a livello informatico.
Essa prevede le seguenti attività:
• registrazione con trattamento delle immagini (acquisizione digitalizzata dei documenti cartacei);
• assegnazione per via telematica al destinatario;
• gestione avanzata della classificazione dei documenti;
• collegamento dei documenti alla gestione dei procedimenti.
A queste può aggiungersi la realizzazione di uno specifico archivio documentale per quei documenti di alto contenuto informativo che meritano uno specifico trattamento (prevedendo ad esempio la creazione di compendi, l'uso di parole chiave per una indicizzazione più dettagliata, ecc.).
La gestione dei flussi di lavoro realizza le seguenti funzionalità (vedasi punto precedente 2.2.4):
• informatizzazione dei processi relativi ai flussi documentali in entrata e in uscita;
• informatizzazione dei processi relativi ai flussi documentali interni;
• integrazione con i flussi di lavoro.
Questa ultima fase è quella che prevede la reingegnerizzazione dei processi dell'Amministrazione al fine di una loro successiva informatizzazione: in particolare vengono gestiti mediante sistemi integrati di flussi di lavoro tutti quei processi che possiedono i requisiti di complessità, ripetitività e stabilità dell'iter.
È evidente che se lo scopo da perseguire è la revisione e la razionalizzazione dei processi amministrativi (Business Process Reengeneering), il raggiungimento di tale obiettivo è propedeutico per l'attuazione anche del Progetto Protocollo e Gestione documentale.
Per poter affrontare i problemi specifici di una corretta gestione elettronica dei documenti, è opportuno analizzare, in sintesi, natura e finalità del sistema documentario, nonché le attività principali che lo caratterizzano, a cominciare dal concetto e dalla funzione del documento, dalla definizione di sistema documentario e di archivio, dall'analisi delle principali funzioni che caratterizzano nel modello organizzativo e normativo italiano la *formazione dei documenti* (registrazione dei documenti e registrazione di protocollo, classificazione d'archivio), nonché la *tenuta degli archivi* e gli *aspetti organizzativi* (le funzioni del Servizio per la tenuta dei documenti e degli archivi, il manuale di gestione previsto dalle regole tecniche del *D.P.R. n. 428 del 1998)*.
Nella più recente attività normativa italiana, a partire dalla *legge n. 241 del 1990*, il *documento* è definito in quanto rappresentazione del contenuto di atti. L'elemento qualificante dell'entità documentaria (cioè la ragione della sua produzione e tenuta) è, infatti, costituito dalla relazione con l'attività amministrativa e pratica cui partecipa in quanto strumento di memorizzazione stabile nel tempo e nello spazio.
I requisiti per l'adozione del protocollo informatico ed il trattamento elettronico dei procedimenti amministrativi riguardano il documento informatico, il formato dei documenti informatici, la firma digitale, l'archiviazione dei documenti, l'accesso telematico, la sicurezza.
I requisiti vincolano le Amministrazioni non solo sul piano organizzativo e tecnologico ma anche per quanto attiene le acquisizioni dei relativi servizi e tecnologie tramite le procedure di appalto.
I requisiti definiti dal legislatore riguardano:
• i documenti informatici;
• i formati relativi ai documenti informatici;
• la firma digitale nei documenti informatici;
• la gestione informatica dei documenti;
• la gestione dei flussi documentali.
5.1 Requisiti dei documenti informatici
La formazione e la conservazione dei documenti informatici delle Pubbliche Amministrazioni (art. 3 della deliberazione Aipa n. 51/2000) devono essere effettuate secondo i seguenti requisiti:
• identificabilità del soggetto che ha formato il documento informatico e dell'amministrazione di riferimento;
• sottoscrizione, quando prescritta, dei documenti informatici tramite la firma digitale ai sensi del *D.Lgs. n. 10 del 2002* e delle vigenti norme tecniche;
• idoneità dei documenti ad essere gestiti mediante strumenti informatici e ad essere registrati mediante il protocollo informatico, ai sensi del *D.P.R. n. 445 del 2000*;
• accessibilità ai documenti informatici tramite sistemi informativi automatizzati;
• leggibilità dei documenti;
• interscambiabilità dei documenti.

Il legislatore sottolinea che solo l'esistenza di tutti i requisiti rende validi e rilevanti i documenti a tutti gli effetti di legge (art. 3, comma 2, della deliberazione Aipa n. 51/2000).
La formazione, e la conservazione non sono considerate dal legislatore solo una operazione tecnologica ma, prima dell'intervento di automazione, il sistema documentale e procedimentale devono essere sottoposti a processi di semplificazione e razionalizzazione (*legge n. 241 del 1990;* art. 3, comma 3, della deliberazione Aipa n. 51/2000).
I contenuti e la struttura dei documenti sono definiti dalla dirigenza e nell'àmbito dell'autonomia delle Amministrazioni, con riferimento all'ordinamento delle stesse (art. 3, comma 4, deliberazione Aipa n. 51/2000).
In particolare, per quanto riguarda le modalità di trasmissione e registrazione dei documenti informatici si rinvia a quanto stabilito dall'art. 15 del *D.P.C.M. 31 ottobre 2000*. Per la leggibilità dei documenti nel tempo si rinvia a quanto stabilito dall'articolo 16 del *D.P.C.M. 31 ottobre 2000* e alla deliberazione Aipa n. 42/2001 che sostituisce la precedente deliberazione n. 24/1998.
5.2 Requisiti relativi ai formati dei documenti informatici.
I formati adottati devono possedere almeno i seguenti requisiti (art. 4 della deliberazione Aipa n. 51/2000):
• consentire, nei diversi àmbiti di applicazione e per le diverse tipologie di trattazione, l'archiviazione, la facilità di lettura, l'interoperabilità e l'interscambio dei documenti;
• la non alterabilità del documento durante le fasi di accesso e di conservazione;
• la possibilità di effettuare operazioni di ricerca tramite indici di classificazione e di archiviazione, nonché sui contenuti dei documenti;
• l'immutabilità nel tempo del contenuto e della sua struttura (per cui i documenti informatici non devono contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificarne la struttura o il contenuto);
• la possibilità di integrare il documento informatico con immagini, suoni e video, purché incorporati in modo irreversibile e nel rispetto dei requisiti di cui alle lettere *b)* e *d)* della citata deliberazione.
5.3 Sistemi di identificazione ed autenticazione
Per la formazione e la gestione di documenti informatici per i quali non è prevista la sottoscrizione, le Pubbliche Amministrazioni possono utilizzare sistemi elettronici di identificazione ed autenticazione nell'àmbito della propria autonomia organizzativa e dei processi di razionalizzazione (art. 5, comma 3, della deliberazione Aipa n. 51/2000).
5.4 Conservazione ed esibizione dei documenti informatici
Per la conservazione e la esibizione dei documenti informatici (art. 7 della deliberazione Aipa n. 51/2000) si applicano le norme di cui alla deliberazione Aipa n. 42/2001 e agli articoli 60 e 61 del *D.P.C.M. 8 febbraio 1999* e successive modificazioni ed integrazioni.
Attraverso la conservazione elettronica dei documenti si eviteranno duplicazioni e accumuli di copie cartacee e verrà favorita la trasformazione graduale degli archivi cartacei della P.A. in sistemi informativi automatizzati ad alto livello di sicurezza ed affidabilità. Inoltre, sarà possibile realizzare sistemi di ricerca più efficaci e più efficienti. Al riguardo si sta ultimando la stesura di un documento rivolto alle Amministrazioni, recante linee guida per l'archiviazione e per la conservazione documentale; tale documento intende ampliare il presente contesto, esaminando anche alcuni aspetti dell'archiviazione e della conservazione digitale strettamente connessi ai processi di archiviazione sostitutiva.
5.5 Requisiti per la gestione informatica dei documenti
Il sistema di gestione informatica dei documenti (art. 52 del *D.P.R. n. 445 del 2000)* deve:
• garantire la sicurezza e l'integrità del sistema;
• garantire la corretta e la puntuale registrazione di protocollo dei documenti in entrata ed in uscita;
• fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'Amministrazione e gli atti dalla stessa formati al fine dell'adozione del provvedimento finale;
• consentire il reperimento delle informazioni riguardanti i documenti registrati;
• consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di «privacy» con particolare riferimento al trattamento dei dati sensibili;
• garantire la corretta organizzazione dei documenti nell'àmbito del sistema di classificazione d'archivio adottato.
Gli interventi sopra indicati esprimono un sistema di gestione documentale di tipo integrato, definito in tutti i suoi aspetti strutturali, funzionali e relazionali sotto il profilo documentale, organizzativo ed informatico. La gestione documentale di questo tipo non può essere delegata solo ai responsabili dei

sistemi informatici; soggetti interessati sono anche i dirigenti e/o i responsabili delle diverse unità organizzative, i quali decidono le regole interne da adottare in materia documentale.

5.6 Requisiti del sistema per la gestione dei flussi documentali

Il sistema per la gestione dei flussi documentali, oltre a possedere i requisiti di cui all'articolo 52 del *D.P.R. n. 445 del 2000*, ai sensi dell'articolo 65 del *D.P.R. n. 445 del 2000*, deve anche:

• fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;

• consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;

• fornire informazioni statistiche sull'attività dell'ufficio;

• consentire lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi.

Tale sistema di gestione dei documenti e dei relativi flussi è di tipo «aperto», totalmente informatico, e deve quindi essere progettato e realizzato in tutte le sue componenti «prima» dell'automazione del sistema stesso. Ciò significa che le amministrazioni devono definire tipologia dei documenti, relazioni tra documenti e procedimenti, struttura dei fascicoli relativi ai procedimenti, iter dei procedimenti stessi, sistemi di ricerca dei documenti e dei fascicoli. Anche in questo caso, non si tratta di una operazione informatica ma di un intervento complesso di tipo documentale, organizzativo, procedurale e tecnico che deve impegnare tutta la dirigenza e/o i responsabili delle unità organizzative.

6. CONTESTO TECNOLOGICO DI RIFERIMENTO.

Al fine di adottare un sistema di protocollo informatico a norma del *D.P.R. n. 445 del 2000*, da parte di ciascuna Amministrazione deve esserne valutato l'impatto sul sistema informativo.

Le indicazioni in merito alla soluzione da adottare dipendono dal contesto specifico. Per le architetture di riferimento si può consultare il documento «Linee guida alla realizzazione dei sistemi di protocollo informatico e gestione dei flussi documentali nelle pubbliche amministrazioni» (GEDOC2), pubblicato dall'Autorità per l'informatica nella pubblica amministrazione nel settembre 2000. Tuttavia, qualunque sia la soluzione tecnologica adottata, si deve tenere presente che il sistema deve essere dotato di alta affidabilità ed in particolare devono essere previste le soluzioni di emergenza in caso di caduta del sistema, in quanto l'applicazione ai processi di lavoro di ciascuna Amministrazione può risultare particolarmente critica (*D.P.C.M. 31 ottobre 2000*, art. 7 - Requisiti minimi di sicurezza dei sistemi di protocollo informatico). A tal fine è necessario approntare un piano e delle procedure di sicurezza (vedasi punto precedente 2.2.2), e le informazioni trattate devono rispondere ai princìpi di riservatezza imposti dalla normativa sulla «privacy».

6.1 Verifica di conformità

Allo scopo di fornire un ausilio alle Amministrazioni nell'attuazione del progetto di automazione della tenuta del protocollo e della gestione elettronica dei documenti ed in particolare nella verifica delle funzionalità dell'applicazione realizzata/acquisita, il Centro di Competenza ha redatto e pubblicato (cfr. http://protocollo.gov.it) il documento «Supporto alla verifica e alla valutazione dei Sistemi di protocollo informatico e di gestione dei flussi documentali», contenente una lista di controllo per la verifica della conformità di tali sistemi ai requisiti desumibili dal quadro di riferimento normativo e tecnologico.

Inoltre, tutte le Amministrazioni, indipendentemente dalla scelta effettuata, possono trovare in tale documento un elenco di requisiti di tipo organizzativo che specifica il contesto organizzativo e di processo coerente con l'introduzione del sistema di protocollo informatico.

6.2 Servizio di gestione del protocollo informatico e dei flussi documentali in modalità ASP

Al fine di fornire ulteriori strumenti per l'attuazione della normativa sulla gestione elettronica dei documenti, il Centro Tecnico per la R.U.P.A. ha promosso la realizzazione di un servizio di gestione del protocollo informatico e dei flussi documentali in modalità ASP per le pubbliche amministrazioni. Con questo obiettivo il Centro tecnico, avvalendosi della Consip nella funzione di stazione appaltante, ha in corso di espletamento, la procedura di gara per l'affidamento del servizio ad operatori di mercato (vedasi bando per la procedura di gara ristretta pubblicato sul sito http://protocollo.gov.it).

Il servizio offerto alle Amministrazioni si articola in:

- REPRO - Gestione nucleo minimo protocollo
- GEDOC - Gestione documentale
- STORE - Archiviazione ottica dei documenti
- Altri servizi accessori tra cui servizi di supporto, consulenza organizzativa (BPR); formazione.

La fornitura sarà regolata da un contratto quadro stipulato tra il fornitore aggiudicatario e il Centro Tecnico per la R.U.P.A. della durata di 48 mesi prorogabile per ulteriori 24 mesi. Tale servizio è rivolto a tutte le Pubbliche Amministrazioni previste dal *decreto legislativo n. 165 del 2001* che devono

manifestare al Centro Tecnico la loro volontà di aderire attraverso la sottoscrizione di una specifica convenzione pubblicata sul sito http://protocollo.gov.it. Le Amministrazioni potranno usufruire del servizio emettendo specifici «Ordinativi di fornitura» nell'àmbito del contratto quadro, sottoscritto dal Centro Tecnico con il fornitore aggiudicatario.
L'Amministrazione aderente potrà usufruire in modo flessibile di qualsiasi servizio tra quelli previsti dalla fornitura con il solo vincolo di aderire al servizio REPRO per un periodo di almeno 24 mesi. I servizi GEDOC, STORE e gli altri servizi accessori, potranno essere richiesti solo dopo aver aderito al servizio di base REPRO. Alla scadenza del contratto verrà fornito all'Amministrazione il software applicativo e la relativa documentazione.
Qualora l'adesione delle Amministrazioni superi i massimali previsti per la fornitura in corso di aggiudicazione, il Centro Tecnico provvederà a bandire ulteriori gare per l'aggiudicazione di nuove forniture. In tal caso, in caso si manifesti l'esigenza da parte di gruppi di Amministrazioni locali aggregate a livello territoriale, il Centro Tecnico potrà verificare la possibilità di specializzare la fornitura sul territorio, favorendo la gestione locale di analoghe iniziative.
Il servizio proposto è fortemente innovativo in quanto, in attuazione delle norme finalizzate alla semplificazione dei procedimenti amministrativi, applica il principio del «riuso» del software di proprietà del Ministero dell'economia e delle finanze e si avvale per la prima volta di un servizio erogato in modalità ASP. Tali scelte permettono, da un lato, di rendere disponibile il servizio in tempi rapidi, dall'altro, di limitare i costi a carico delle Amministrazioni a quelli relativi all'effettivo utilizzo del servizio (costi a consumo).
6.3 Interoperabilità dei sistemi di protocollo
La *circolare 7 maggio 2001* Aipa recepisce le indicazioni presenti nel *D.P.R. n. 445 del 2000* e fornisce le regole tecniche per l'interoperabilità dei sistemi di protocollo, ossia per il «trattamento automatico, da parte di un sistema di protocollo ricevente, delle informazioni trasmesse da un sistema di protocollo mittente, allo scopo di automatizzare le attività ed i processi amministrativi conseguenti».
Il Centro Tecnico rende disponibili alcune caselle di posta elettronica da utilizzate per effettuare i test di interoperabilità dei sistemi di protocollo informatico.
6.4 Posta certificata
Laddove lo scambio dei flussi comporta uno scambio documentale lo strumento tecnico a supporto è la posta certificata. Quest'ultima, ai sensi dell'articolo 14 del *D.P.R. n. 445 del 2000*, è un servizio di messaggistica che, attraverso l'utilizzo dei relativi standard, è in grado di fornire ricevute di recapito. Le stesse, firmate elettronicamente dal sistema emittente, sono messaggi generati automaticamente dal servizio di posta certificata, recanti una serie di informazioni che caratterizzano l'evento cui sono associate. Ulteriori funzionalità accessorie riguardano la garanzia della confidenzialità, dell'integrità, e della storicizzazione delle ricevute di recapito. Il servizio di posta certificata è strettamente correlato all'Indice della PA, poiché in esso sono pubblicati gli indirizzi di posta certificata associati alle AOO e alle funzioni organizzative eventualmente previste dalle Amministrazioni.
6.5 Cooperazione applicativa
Tra gli obiettivi del piano d'azione di *e-government*, necessari a mettere in atto procedure di trasparenza degli atti amministrativi, l'erogazione di servizi integrati ai cittadini e alle imprese implica l'integrazione tra i servizi di diverse Amministrazioni.
Sul piano tecnologico ciò si traduce nell'adozione di uno standard comune per le singole interazioni tra le Pubbliche Amministrazioni, definito nella busta di e-government allegata al relativo Bando e nelle successive specifiche indicazioni che verranno fornite da parte del Centro tecnico per la R.U.P.A.

Direttiva in materia di trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.

NUMERO SCHEDA: 2139

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: PROTOCOLLO INFORMATICO

NATURA ATTO: DIRETTIVA

DATA ATTO: 09/12/2002

ORGANO: MINISTERI

In data 9 dicembre 2002 è stata emanata, d'intesa tra il Ministero per l'Innovazione e le Tecnologie, ed il Ministero per la Funzione Pubblica, la direttiva "Trasparenza dell'azione amministrativa e gestione dei flussi documentali", la quale prevede che, entro il primo gennaio 2004, le Pubbliche Amministrazioni dovranno adottare il sistema di gestione e di archiviazione elettronica di tutti i documenti. Scopo della direttiva è di promuovere l'adozione del protocollo informatico in tutte le amministrazioni centrali e negli Enti pubblici non economici, favorendo, in tal modo, l'utilizzo esteso di documenti informatici e l'erogazione di servizi in rete a cittadini ed imprese, che potranno verificare lo stato delle pratiche collegandosi ai siti della pubblica amministrazione.
L'eliminazione dei registri cartacei e la razionalizzazione dei flussi documentali determinerà, infatti, un aumento dell'efficienza interna degli uffici poiché tale modalità consentirà di trasformare le pratiche presentate agli uffici pubblici in documenti digitali, permettendo la trasmissione e la gestione interna della pratica per via telematica ed eliminando il trasferimento "materiale" del fascicolo cartaceo.
La Direttiva, in accordo con il "Piano nazionale di e-Government", intende, infatti, assicurare il più rapido e proficuo utilizzo della firma elettronica nello scambio di documenti e atti tra le amministrazioni.

Si allega il testo della direttiva.

Dir.Min. 9 dicembre 2002

Trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali.

PREMESSA.
La presente direttiva è indirizzata a tutte le amministrazioni centrali dello Stato e agli enti pubblici sottoposti alla vigilanza ministeriale. Per le regioni e gli enti locali e territoriali costituisce contributo alle determinazioni in materia, nel rispetto della loro autonomia amministrativa. Può rappresentare schema di riferimento anche per le altre amministrazioni pubbliche di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165.
Il legislatore ha in questi anni emanato diverse norme volte a regolare gli aspetti concernenti la gestione elettronica dei documenti amministrativi per attuare la legge n. 59 del 1997 che ha dato validità giuridica al documento informatico; tale attività normativa ha portato alla emanazione di norme disciplinanti sia la firma digitale (decreto del Presidente della Repubblica n. 513 del 1997 e relative regole tecniche di cui al decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999); sia la tenuta dei sistemi di protocollo informatico (decreto del Presidente della Repubblica n. 428 del 1998 e relative regole tecniche di cui al decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000). Tali norme, ad eccezione di quelle recanti le citate «regole tecniche», sono poi confluite nel testo unico sulla documentazione amministrativa (decreto del Presidente della Repubblica n. 445 del 2000). Ulteriori norme sono state emesse per garantire la interoperabilità dei sistemi di protocollo (Circolare 7 maggio 2001, n. AIPA/CR/28). Dal punto di vista della archiviazione del documento elettronico è stata emanata nel luglio del 1998 la deliberazione n. 24 del 1998 successivamente sostituita dalla deliberazione n. 42 del 2001; tale deliberazione si propone lo scopo di regolare la fase di conservazione dei documenti conformi alle normative precedentemente citate. Infine è stato emanato il decreto legislativo 23 gennaio

2002, n. 10, recante l'attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche che rende la normativa italiana sulla firma elettronica coerente con quella europea; fra le disposizioni citate si ritiene utile ricordare in particolare quelle concernenti i requisiti dei sistemi di cui agli articoli 52, 53, 55 e 56 del decreto del Presidente della Repubblica n. 445 del 2000 ed all'art. 7 decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000.
Il decreto del Presidente della Repubblica n. 445 del 2000 fissa al 1° gennaio 2004 il termine per la realizzazione dei sistemi finalizzati alla gestione del protocollo informatico e dei procedimenti amministrativi, lasciando a ciascuna amministrazione la scelta delle modalità organizzative e delle soluzioni tecnologiche da adottare.
Considerato il grande impatto sull'organizzazione delle amministrazioni ed in particolare sui sistemi di gestione dei flussi documentali è necessario che tutte le amministrazioni provvedano per tempo alla individuazione delle aree organizzative omogenee (art. 50 del decreto del Presidente della Repubblica n. 445 del 2000), come peraltro richiamato dalla Dir.Min. 21 dicembre 2001, «Linee guida in materia di digitalizzazione dell'amministrazione» emanata dal Ministro per l'innovazione e le tecnologie, pubblicata nella Gazzetta Ufficiale - serie generale - del 5 febbraio 2002, n. 30, che ha sottolineato l'importanza del tema della trasparenza dell'azione amministrativa, intesa, in questo contesto, come concreto diritto del cittadino e dell'impresa di conoscere lo stato delle attività amministrative che li riguardano e avere la garanzia che tali attività siano condotte nel rispetto di regole di priorità e massimo impegno, nonché le opportunità che i sistemi di gestione del protocollo informatico offrono al riguardo.
Inoltre si ricorda che il Comitato dei Ministri per la Società dell'informazione ha approvato, il 13 febbraio 2002, un documento in cui sono stati definiti i dieci obiettivi fondamentali di legislatura, uno dei quali ha riguardato il tema della trasparenza dell'azione amministrativa. Tale obiettivo è coerente con il principio che l'azione delle amministrazioni debba essere guidata dalle esigenze degli utenti.
OBIETTIVI.
L'obiettivo primario di questa direttiva è quello di promuovere in tutte le amministrazioni centrali e gli enti pubblici sottoposti alla vigilanza ministeriale la realizzazione di sistemi informativi per la gestione elettronica dei flussi documentali.
Ciò allo scopo di assicurare il più rapido e proficuo utilizzo del documento informatico e della firma elettronica negli scambi di documenti ed atti tra amministrazioni, in coerenza con i rispettivi obiettivi istituzionali e con gli obiettivi strategici di digitalizzazione della pubblica amministrazione.
Il protocollo informatico e, più in generale, la gestione elettronica dei flussi documentali hanno la finalità di migliorare l'efficienza interna degli uffici attraverso l'eliminazione dei registri cartacei, la riduzione degli uffici di protocollo e la razionalizzazione dei flussi documentali. Inoltre con tali sistemi ci si prefigge di migliorare la trasparenza dell'azione amministrativa attraverso strumenti che consentano l'accesso allo stato dei procedimenti ed ai relativi documenti da parte di cittadini, imprese ed altre amministrazioni.
Per conseguire tali obiettivi è necessario che le amministrazioni, oltre ad ottemperare a quanto stabilito dalla normativa vigente (cd. «nucleo minimo», articoli 55 e 56 del decreto del Presidente della Repubblica n. 445 del 2000), provvedano ad avviare progetti destinati a diffondere l'utilizzo di documenti elettronici sia al loro interno che negli scambi con i soggetti esterni, con lo scopo di facilitare e favorire l'accesso alle informazioni disponibili sui procedimenti e sui documenti protocollati.
INTEROPERABILITÀ E FLUSSI DOCUMENTALI.
L'azione coordinata di interventi che definiscono il quadro normativo e progettuale del nuovo sistema di gestione elettronica dei documenti ha prodotto:
la realizzazione da parte del Centro tecnico per la rete unitaria della pubblica amministrazione di un indice delle pubbliche amministrazioni (IPA) come previsto dal decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000; informazioni in proposito si trovano sul sito http//indicepa.gov.it;
la realizzazione di un sistema di posta elettronica certificata, cioè di un sistema che certifichi l'identificazione univoca del mittente e del destinatario e la ricezione del messaggio da parte di quest'ultimo, ai sensi del decreto del Presidente della Repubblica n. 445 del 2000, art. 14, allo scopo di fornire, nell'immediato, alle amministrazioni uno strumento sicuro di scambio di messaggi ufficiali e, in prospettiva, al cittadino e all'impresa un canale aggiuntivo di comunicazione con la pubblica amministrazione caratterizzato da rapidità ed efficienza.
Premesso che lo sviluppo di strumenti quali la firma elettronica ed il protocollo informatico, integrati con servizi di interoperabilità, rende possibile la realizzazione effettiva di una gestione completamente automatizzata dei flussi documentali, si ricorda che, nell'àmbito di una comunicazione tra i sistemi di protocollo di differenti amministrazioni, o tra differenti sistemi di protocollo della stessa

amministrazione, si ritiene garantita la interoperabilità tra detti sistemi quando è consentito al sistema ricevente di trattare automaticamente le informazioni trasmesse dal sistema mittente.
Su tale tematica è possibile fare riferimento al testo del titolo «Interoperabilità dei sistemi di protocollo informatico in ambiente distribuito» emanato dall'Aipa e disponibile sul sito web http://protocollo.gov.it dedicato alla tematica oggetto della presente direttiva.
IMPLICAZIONI OPERATIVE PER LE AMMINISTRAZIONI.
Al fine di attuare la normativa vigente e usufruire dei servizi resi disponibili dal Centro tecnico, è necessario che le amministrazioni nei prossimi mesi svolgano un articolato insieme di azioni nell'àmbito della gestione elettronica dei documenti e della trasparenza amministrativa, azioni che sono di seguito descritte.
LA GESTIONE ELETTRONICA DEI DOCUMENTI.
Per i sistemi di gestione elettronica dei documenti è necessario:
individuare le aree organizzative omogenee (AOO) e i relativi uffici di riferimento ai sensi dell'art. 50, comma 4, del decreto del Presidente della Repubblica n. 445 del 2000;
comunicare al Centro tecnico la casella ufficiale di posta elettronica per l'iscrizione delle AOO nell'indice delle P.A.; indicazioni operative in tal senso saranno inviate dal Centro tecnico e sono presenti sul sito http://indicepa.gov.it;
comunicare al Centro tecnico, per ogni AOO istituita, il nominativo del responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'art. 61, comma 2, del decreto del Presidente della Repubblica n. 445 del 2000;
adottare, per ogni AOO istituita, il manuale di gestione come previsto dalle regole tecniche (art. 5 del decreto del Presidente del Consiglio dei Ministri 31 ottobre 2000;)
pubblicare e rendere accessibile tramite internet il manuale di gestione che descrive il sistema di gestione e di conservazione dei documenti e fornisce le istruzioni necessarie per il corretto funzionamento del servizio per la tenuta del protocollo informatico. Il manuale comprende analisi, decisioni, piani, iter delle attività, classificazioni, ecc., definiti in relazione alle specificità organizzative, funzionali, strutturali e di servizio dell'amministrazione di riferimento; assumono particolare rilievo le disposizioni in merito alla pianificazione degli interventi, alla gestione ed all'iter di lavorazione dei documenti, dei sistemi di classificazione ed alle modalità di accesso;
predisporre un progetto operativo per la progressiva messa in opera di sistemi di protocollo informatico integrati con la posta elettronica certificata e la firma elettronica ai sensi dell'art. 10, comma 3, del decreto del Presidente della Repubblica n. 445 del 2000 nel rispetto dei princìpi di interoperabilità di cui alla circolare 7 maggio 2001, n. AIPA/CR/28;
predisporre correlate attività di formazione d'intesa con il Dipartimento della funzione pubblica ai sensi della Dir.Min. 13 dicembre 2001 del Ministro della funzione pubblica sulla formazione;
fornire informazioni al Centro tecnico sullo stato di avanzamento dei progetti al fine di permettere delle rilevazioni periodiche sullo stato di attuazione della normativa.
È necessario che le amministrazioni completino le attività precedentemente descritte entro il 31 maggio 2003.
A questo fine le amministrazioni in indirizzo definiscono un piano d'azione dettagliato che preveda lo svolgimento delle attività su elencate tenendo conto della scadenza del 1° gennaio 2004 prevista dal decreto del Presidente della Repubblica n. 445 del 2000 per l'adozione del sistema di protocollo informatico e di comunicare, entro il 28 febbraio 2003, tale piano d'azione al Centro tecnico.
LA TRASPARENZA AMMINISTRATIVA.
Per l'attuazione della trasparenza dell'attività amministrativa, così come intesa da questa normativa, le amministrazioni svolgono, entro il 28 febbraio 2003, le seguenti azioni:
comunicare al Centro tecnico il nome di un referente, al fine di definire le attività di interesse comune e concordare i relativi tempi di realizzazione;
individuare i servizi di propria competenza erogati ai cittadini e alle imprese sia con modalità tradizionali che in rete;
pianificare, secondo criteri di priorità, l'attuazione della trasparenza dell'azione amministrativa come definita in precedenza, tramite la predisposizione di progetti orientati a fornire ai cittadini e alle imprese servizi informativi attraverso canali telematici diretti o tramite intermediazione dell'Ufficio relazioni con il pubblico;
migliorare la comunicazione tra gli uffici e gli URP al fine di migliorare la comunicazione esterna e l'esercizio del diritto di accesso;

compilare, per ogni progetto una scheda informativa, secondo lo schema riportato in allegato 1, da inviare al Centro tecnico. La scheda contiene gli elementi informativi essenziali per pianificare l'attuazione del progetto di trasparenza.

IL RUOLO DEL CENTRO TECNICO E DEL CENTRO DI COMPETENZA PER IL PROGETTO PROTOCOLLO INFORMATICO E TRASPARENZA AMMINISTRATIVA.

Il Centro tecnico, continuando le attività svolte fin qui dall'AIPA, ha istituito un centro di competenza per il progetto protocollo informatico e trasparenza amministrativa, quale unico punto di riferimento, che svolgerà funzioni di indirizzo e coordinamento e promuoverà iniziative di affiancamento per garantire l'attuazione della presente direttiva, in particolare attraverso:

le informazioni, le esperienze e i servizi messi a disposizione tramite il sito web sulla gestione elettronica dei documenti http://protocollo.gov.it;

la collaborazione che sarà fornita dal centro di competenza, che può essere contattato al seguente indirizzo di posta elettronica: protocollo@gov.it.

Allegato 1

Scheda per l'individuazione dei progetti di trasparenza amministrativa

Compilare, per ogni progetto di trasparenza, una scheda informativa da inviare al Centro tecnico presso il centro di competenza del progetto protocollo informatico e trasparenza amministrativa che contenga:

la denominazione del progetto;

il nome dell'amministrazione e del referente;

la data indicativa di erogazione del servizio di trasparenza;

la denominazione dei procedimenti amministrativi oggetto di trasparenza e una descrizione del loro iter; per ogni procedimento amministrativo, la denominazione dell'ufficio responsabile e l'insieme delle fasi di cui è reso possibile conoscere lo stato.

Tali informazioni potranno essere fornite secondo il seguente schema.

Tabella 1

Progetto di trasparenza

Per ogni progetto di trasparenza indicare la denominazione del progetto, la denominazione dell'amministrazione proponente, il referente del progetto e la data indicativa in cui l'amministrazione intende fornire il servizio di trasparenza.

				Data indicativa di
				erogazione del
Num.	Denominazione progetto	Amministrazione/Ente	Referente	servizio di
				trasparenza
				(mese e anno)
1	Esempio: Invalidità civile	Esempio: Ministero dell'economia e delle		
		finanze. Dipartimento direzione generale		
		dei servizi vari e delle pensioni di guerra -		
		Divisione XI		
2				
...				

Tabella 2

Procedimenti amministrativi
Riportare la denominazione, una descrizione dell'iter del procedimento amministrativo oggetto del progetto di trasparenza e la denominazione dell'ufficio responsabile.

Num.	Denominazione procedimento amministrativo	Descrizione e indicazione della struttura responsabile	Ufficio responsabile
1	Esempio: Ricorsi pensioni di invalidità civile	Esempio: Richiesta del riconoscimento di una invalidità civile. Verbale negativo da parte della ASL competente. Ricorso avverso la decisione presso il MEF entro sessanta giorni. Esame della documentazione ed eventuale richiesta di ulteriore documentazione effettuata da parte dell'ufficio XIII se la prima fase ha esito positivo si passa ad una seconda fase, gestita dall'ufficio XIV, che prevede l'effettuazione di ulteriori verifiche mediche, da parte di apposita commissione. Emissione di un nuovo verbale. Il verbale torna successivamente all'Ufficio XIII che predispone il provvedimento finale di accoglimento o rigetto del ricorso.	Esempio: Direzione generale dei servizi vari e delle pensioni di guerra – Divisione XI
2			
...			

Tabella 3
Procedimenti-Fasi
Nell'àmbito dell'iter del procedimento amministrativo, definire le fasi di cui è possibile conoscere lo stato. Ad esempio, per un procedimento di richiesta di contributi l'amministrazione potrebbe decidere di far conoscere lo stato delle seguenti fasi: ricezione, istruttoria, delibera.

Num.	Denominazione procedimento	Insieme delle fasi
1	Esempio: richiesta di contributi	Esempio: ricezione - istruttoria - delibera
2		

Gestione informatica dei documenti: le direttive di Palazzo Chigi agli uffici.

NUMERO SCHEDA: 849

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: PROTOCOLLO INFORMATICO

FONTE: GUIDA AGLI ENTI LOCALI

NUMERO: 6

DATA: 19/02/2000

PAGINA: 28-37

RIFERIMENTO NORMATIVO: Dpr 428/98; L. 59/97

NATURA ATTO: DIRETTIVA

DATA ATTO: 28/10/1999

ORGANO: CONSIGLIO DEI MINISTRI

La direttiva del Presidente del Consiglio dei ministri del 28/10/99 si riferisce alla necessità di un'organizzazione omogenea nel processo di gestione del protocollo informatico da parte della P.A, cosi' come disposto dal Dpr. 428/98.
La direttiva mira pertanto a uniformare le procedure di attuazione, prescrivendo l'individuazione, da parte degli organi di direzione politica, di specifiche strutture o gruppi di lavoro e indica i compiti da affidare.
Secondo la direttiva, per la determinazione delle aree occorrera' individuare i settori dell'amministrazione con esigenze di gestione della documentazioine omogenee.
La direttiva ha come destinatari le amministrazioni statali e gli enti pubblici sottoposti a vigilanza ministeriale; per le Regioni e gli Enti locali, invece, si pone come contributo alle determinazioni in materia, nel rispetto della loro autonomia amministrativa che dovra' comunque esplicarsi nell'ambito delle linee generali dettate dal Dpr 428/98

Si allega il testo integrale della direttiva.

Dir.P.C.M. 28 ottobre 1999
Gestione informatica dei flussi documentali nelle pubbliche amministrazioni

1. Premessa.

Nel processo di generale e continua trasformazione delle pubbliche amministrazioni, l'innovazione tecnologica rappresenta un fattore di sviluppo e di razionalizzazione, oltre che di contenimento dei costi di funzionamento e di miglioramento dei servizi resi al cittadino-utente.
Perché tale cambiamento produca risultati effettivi è, tuttavia, indispensabile, da un lato, disporre di infrastrutture evolute, dall'altro, realizzare un'efficace azione di coordinamento, sia sul piano amministrativo-organizzativo che su quello tecnico-informatico, anche mediante l'adozione di direttive ed indirizzi in materia e di regole tecniche comuni ed aggiornate.
Occorre, inoltre, un ulteriore sforzo organizzativo, professionale e culturale che consenta di passare dalla concezione tradizionale di sistema informatico a quella di sistema informativo, consistente in un

flusso di informazioni continuo e pluridirezionale, finalizzato a fornire il supporto conoscitivo alle attività decisionali.
Allorché, difatti, la gestione dell'insieme dei flussi informativi e, in particolare, documentali, viene affidata alla tecnologia informatica e telematica, questa non si presenta più quale mero strumento tecnico di automazione delle attività di ufficio (office automation) ma come vera e propria risorsa strategica, necessaria per la migliore efficacia delle politiche della singola amministrazione.
In questa prospettiva, i sistemi di protocollo informatico, nella loro versione più evoluta, comprendono talune funzioni innovative per la pubblica amministrazione. Oltre alla possibilità di protocollare i tradizionali documenti cartacei, è possibile anche: protocollare documenti elettronici; collegare direttamente al sistema di protocollo il sistema di archiviazione e conservazione dei documenti; garantire forme più efficaci di accesso agli atti amministrativi; fornire elementi utili ai fini delle attività di controllo di gestione; sperimentare applicazioni elettroniche della gestione dei flussi documentali (workflow) e del telelavoro.
La gestione elettronica dei flussi documentali nell'ambito delle pubbliche amministrazioni risulta così finalizzata - oltre che al potenziamento dei supporti conoscitivi - al miglioramento dei servizi, alla trasparenza dell'azione amministrativa e al contenimento dei costi, secondo criteri di economicità, efficacia e pubblicità dell'azione amministrativa.
2. Quadro normativo e tecnico.
Nel periodo 1997-1999 è stata condotta un'azione coordinata di interventi che definiscono il quadro normativo e tecnico del nuovo sistema di gestione elettronica delle attività amministrative:
l'art. 15, comma 2, della legge 15 marzo 1997, n. 59, che prevede che gli atti, dati e documenti, formati dalla pubblica amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge;
il decreto del Presidente della Repubblica 10 novembre 1997, n. 513, «Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art. 15, comma 2, della legge 15 marzo 1997, n. 59»;
l'art. 4 della legge 16 giugno 1998, n. 191, e il relativo regolamento emanato con decreto del Presidente della Repubblica 8 marzo 1999, n. 70, in materia di telelavoro nelle pubbliche amministrazioni;
la delibera dell'AIPA 30 luglio 1998, n. 24, che definisce le regole tecniche sull'archiviazione ottica;
il decreto del Presidente della Repubblica 20 ottobre 1998, n. 428, recante «Regolamento per la tenuta del protocollo amministrativo con procedura informatica», che fissa criteri e modalità per la gestione elettronica dei documenti, consente la interoperabilità tra le amministrazioni pubbliche e l'accesso esterno al sistema documentario, compatibilmente con le norme sulla tutela dei dati personali;
il decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999, recante le «Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513»;
la circolare dell'Autorità per l'informatica nella pubblica amministrazione (AIPA) 26 luglio 1999, n. 22, che detta le modalità per presentare le domande di iscrizione nell'elenco pubblico dei certificatori;
Il quadro normativo e tecnico sarà completato - a norma dell'art. 4, comma 4, del decreto del Presidente della Repubblica 20 ottobre 1998, n. 428 - con l'imminente emanazione delle regole e criteri relativi alle operazioni di registrazione di protocollo.
3. Coordinamento amministrativo e tecnico.
Il coordinamento delle iniziative - sia all'interno dell'amministrazione, sia tra le diverse amministrazioni - costituisce, senza dubbio, un fattore critico di successo del processo di innovazione in atto.
È necessario, pertanto, che ciascuna amministrazione individui strutture di coordinamento esistenti o istituisca specifiche strutture o gruppi di lavoro cui affidare l'attuazione della normativa indicata, con particolare riferimento allo sviluppo di sistemi di protocollo e di gestione informatica dei documenti.
La piena responsabilità e sensibilità da parte degli organi di vertice delle amministrazioni è indispensabile per l'attuazione di soluzioni che incideranno anche profondamente sul tessuto organizzativo.
A tal fine è necessario, in sede di definizione delle priorità e degli obiettivi ai sensi dell'art. 3, comma 1, lettera b), del decreto legislativo 3 febbraio 1993, n. 29, che si proceda da parte degli organi di direzione politica ad attribuire alle sopra indicate strutture, specifici obiettivi finalizzati all'attuazione della presente direttiva. I risultati ottenuti nell'esecuzione dei progetti relativi a detti obiettivi saranno valutati ai fini della corresponsione delle indennità di risultato.

Tra i compiti da affidare alle strutture di coordinamento o ai gruppi di lavoro dovranno essere inclusi i seguenti:
indicazione dei principali interventi di trasformazione organizzativa da introdurre ai fini dell'automazione della gestione documentale (individuazione delle grandi aree organizzative omogenee; costituzione dei servizi per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi; individuazione delle risorse umane da qualificare ai fini dell'automazione della gestione documentaria);
elaborazione di piani integrati e coordinati di classificazione e conservazione che assicurino il rispetto di criteri uniformi per ciascuna amministrazione e definizione dei costi di realizzazione e dei benefici organizzativi e operativi che derivano dall'attuazione del nuovo sistema di gestione elettronica dei documenti;
elaborazione di programmi di gestione del cambiamento organizzativo a supporto dell'innovazione tecnologica;
definizione di sistemi di monitoraggio specifico volti alla verifica dello stato di attuazione dei progetti e alla valutazione dei risultati ottenuti in termini di contenimento dei costi e di aumento dell'efficienza e dell'efficacia dell'azione amministrativa.
Ai fini dell'attuazione della presente direttiva e per il coordinamento delle conseguenti iniziative, presso la Presidenza del Consiglio dei Ministri è istituito un apposito organismo, denominato «Comitato per l'innovazione tecnologica nelle procedure amministrative» con i seguenti compiti:
assicurare pieno coordinamento per l'attuazione delle iniziative oggetto della presente direttiva, anche mediante l'adozione di indirizzi e criteri guida destinati alle strutture di coordinamento individuate presso ciascuna amministrazione;
dare impulso alle attività progettuali e organizzative necessarie;
diffondere informazioni e documentazione sulle esperienze più significative;
svolgere attività di monitoraggio sui progetti già realizzati o in corso di realizzazione.
Il comitato sarà composto da rappresentanti della Presidenza del Consiglio dei Ministri - Segretariato generale, del Dipartimento per la funzione pubblica, dell'AIPA, del Ministero dei beni e delle attività culturali e della Conferenza unificata.
4. Adempimenti delle amministrazioni.
L'attuazione dell'iniziativa presuppone che le amministrazioni, oltre a predisporre le opportune risorse tecnologiche, avviino cambiamenti di natura strutturale e organizzativa, che includono:
l'individuazione e la nomina tra i dirigenti e i funzionari in organico di un responsabile del protocollo informatico, ai sensi dell'art. 12, comma 2, del decreto del Presidente della Repubblica n. 428 del 1998, in possesso di idonei requisiti professionali o di professionalità tecnico-archivistica e, naturalmente, di un'adeguata sensibilità all'utilizzo delle tecnologie informatiche;
l'individuazione - prevista dall'art. 2, comma 2, del decreto del Presidente della Repubblica n. 428 del 1998, citato - delle grandi aree organizzative omogenee nel cui ambito operi un unico sistema di protocollo;
la costituzione, prevista dall'art. 12 del medesimo decreto, di una specifica struttura per la gestione del protocollo informatico (il «Servizio per la tenuta del protocollo informatico e la gestione dei flussi documentali e degli archivi»);
l'attivazione di un capillare programma di sensibilizzazione e di formazione, che in questo contesto assume un rilevante significato culturale.
Le amministrazioni sono quindi chiamate a intervenire direttamente nella fase attuativa del decreto del Presidente della Repubblica n. 428 del 1998 per lo sviluppo del «governo elettronico» nelle pubbliche amministrazioni, anche nella prospettiva del loro effettivo ingresso nella rete unitaria delle pubbliche amministrazioni.
Il raggiungimento degli obiettivi indicati dipende, innanzi tutto, dalla capacità di progettare in ciascuna amministrazione un vero e proprio programma di interventi di natura organizzativa e tecnologica, correttamente dimensionato alle effettive esigenze operative.
5. La definizione delle grandi aree organizzative omogenee.
Per la corretta determinazione delle aree di cui all'art. 2, comma 2, del decreto del Presidente della Repubblica n. 428 del 1998 è necessario individuare settori dell'amministrazione che, per tipologia di mandato istituzionale, di funzione amministrativa perseguita, di obiettivi e di attività svolta, presentino esigenze di gestione della documentazione tendenzialmente omogenee.
Ciascuna amministrazione valuterà la rispondenza delle strutture esistenti ai criteri di omogeneità da utilizzare ai fini dell'individuazione delle aree.

Gli uffici periferici dello Stato e gli enti locali potranno prevedere un'unica area, salvo casi di particolare complessità organizzativa. In questo modo è possibile arrivare all'attesa diminuzione e semplificazione dell'insieme dei sistemi di protocollo oggi esistenti.
Poiché le varie aree non dovranno essere considerate come aree chiuse sarà necessario definire possibilità e modalità di accesso ai sistemi da parte di utenti esterni, nonché le possibili interazioni tra i sistemi informatici di protocollo e di gestione documentale di aree diverse.
Nei casi in cui un'amministrazione individui al proprio interno diverse aree per la gestione dei flussi documentali, occorre prevedere la possibilità non solo di accedere da ciascuna area a più sistemi di protocollo ma anche di adottare forme di cooperazione tra sistemi, allo scopo di fornire alle varie unità organizzative una visione integrata.
6. Princìpi base in materia di classificazione e fascicolazione dei documenti.
La definizione e l'applicazione di sistemi di classificazione di archivio - a cura delle singole amministrazioni - rappresentano il presupposto indispensabile per la realizzazione e lo sviluppo dei sistemi di gestione informatica dei flussi documentali. L'obiettivo è la costruzione di un sistema integrato di informazioni sui documenti.
La classificazione si presenta come uno schema generale di voci logiche, articolate in modo tendenzialmente gerarchico e stabilite in modo uniforme, che identificano le funzioni e le attività di ciascuna amministrazione. Tali voci non dovrebbero identificarsi con la struttura organizzativa in quanto quest'ultima può essere soggetta a trasformazioni.
Tra le finalità perseguite dalla classificazione, vi sono:
la definizione dei criteri di formazione e di organizzazione dei fascicoli, dei dossier e delle serie di documenti tipologicamente simili (circolari, verbali, registri contabili ecc.);
il reperimento dei documenti in relazione all'insieme della produzione documentaria riferita ad una specifica attività o ad un procedimento amministrativo;
la realizzazione delle operazioni di selezione dei documenti archivistici ai fini della loro conservazione ovvero della loro distruzione.
Nell'ambito di un'amministrazione o di aree organizzative omogenee della medesima, il sistema di classificazione può prevedere, secondo modalità uniformi:
voci che corrispondono alle funzioni caratterizzanti l'area stessa (voci di primo livello);
voci che identificano le attività per ciascuna funzione (voci di livello successivo);
collegamento con i tempi e le modalità di conservazione dei fascicoli ai sensi dell'art. 19, comma 1, del decreto del Presidente della Repubblica n. 428 del 1998;
eventuale riferimento alle modalità di accesso nel rispetto della tutela dei dati personali.
I livelli finali così definiti costituiranno l'elemento logico di aggregazione di tutti i documenti attinenti ad una medesima tipologia di attività, organizzati in fascicoli relativi a materie, procedimenti, singoli affari nei quali si esplica in concreto l'attività identificata.
7. Rete unitaria delle pubbliche amministrazioni e flussi documentali.
Le nuove prospettive dell'interconnessione e della piena interoperabilità tra i sistemi informativi pubblici - al centro della realizzazione della rete unitaria delle pubbliche amministrazioni - conferiscono una dimensione ancor più ampia agli obiettivi ed agli indirizzi oggetto della presente direttiva che, pertanto, si pone in rapporto di continuità con la direttiva del Presidente del Consiglio dei Ministri 5 settembre 1995, avente ad oggetto la realizzazione dell'infrastruttura telematica pubblica.
In questo quadro il protocollo informatico si caratterizza quale progetto intersettoriale, strettamente connesso all'attuazione della rete unitaria.
In una pubblica amministrazione effettivamente integrata, difatti, gli interlocutori di un sistema di protocollo informatico sono - oltre agli utenti interni all'area organizzativa omogenea a cui il sistema fa riferimento e agli utenti delle altre aree organizzative omogenee - gli utenti esterni all'organizzazione.
Nel documento di indirizzo GEDOC, disponibile sul sito web dell'Autorità per l'informatica (www.aipa.it), tali aspetti sono stati inquadrati nell'ambito della configurazione organizzativa denominata «protocollo federato».
Nel decreto del Presidente della Repubblica n. 428 del 1998 il principio del «non isolamento» dei sistemi di protocollo informatico è affermato con chiarezza negli articoli 10 e 11 riguardanti l'accesso esterno, sia da parte delle altre amministrazioni che dei soggetti esterni interessati ai relativi procedimenti amministrativi.
In particolare, l'accesso esterno tra le pubbliche amministrazioni deve avvenire secondo le modalità di interconnessione stabilite nell'ambito delle norme e dei criteri tecnici emanati per la realizzazione della rete unitaria, in relazione a funzioni minime di accesso fornite dall'amministrazione che gestisce il sistema di protocollo informatico (art. 11).

Per quanto riguarda i soggetti esterni, l'art. 10 del decreto del Presidente della Repubblica n. 428 del 1998 prevede sia un collegamento esplicito tra gli uffici per le relazioni con il pubblico (URP) e il sistema di gestione informatica dei flussi documentali, sia la possibilità di accesso diretto da parte dell'interessato, preceduto quest'ultimo dalla definizione delle modalità tecniche ed organizzative volte a garantire la riservatezza della persona e l'identificazione certa del soggetto che effettua l'accesso (comma 3).

8. Iniziative di formazione professionale in materia.

L'impegno necessario per l'attuazione dei sistemi di gestione dei flussi documentali richiede interventi di riqualificazione e formazione professionale.

Al riguardo l'Autorità per l'informatica nella pubblica amministrazione e il Dipartimento della funzione pubblica, in collaborazione con il Formez provvederanno agli interventi di formazione per le seguenti figure professionali coinvolte nel processo di gestione informatica dei documenti:

responsabili della reingegnerizzazione dei processi legati alla protocollazione informatica;

responsabili degli uffici di protocollo informatico;

operatori di protocollo informatico;

responsabili delle altre strutture utenti del protocollo informatico.

I percorsi formativi previsti per le diverse figure professionali prevedono l'acquisizione delle conoscenze organizzative, archivistiche e informatiche indispensabili per l'utilizzo efficace degli strumenti necessari alla gestione informatizzata dei documenti.

La presente direttiva è indirizzata a tutte le amministrazioni centrali dello Stato e agli enti pubblici sottoposti alla vigilanza ministeriale. Per le regioni e gli enti locali territoriali costituisce contributo alle determinazioni in materia, nel rispetto della loro autonomia amministrativa. Può rappresentare schema di riferimento anche per le altre amministrazioni pubbliche di cui all'art. 1, comma 2, del decreto legislativo 3 febbraio 1993, n. 29.

CAPITOLO VI

CODICE DELL'AMMINISTRAZIONE DIGITALE

Il Codice dell'amministrazione digitale, adottato con decreto legislativo 7 marzo 2005, n. 82, in vigore dal 1° gennaio 2006, accorpa e riordina la normativa in materia di attività digitale delle pubbliche amministrazioni e viene in questa breve premessa illustrato avvalendosi della presentazione "ufficiale" che del Codice viene fatta in un sito ad esso appositamente dedicato, a cura del Ministero per l'Innovazione e le Tecnologie, www.padigitale.it.

Il Codice è il risultato di oltre due anni di lavoro, di continue interazioni con tutti i livelli istituzionali, con le Regioni e le Autonomie Locali. E' stato redatto dal Ministro per l'Innovazione e le Tecnologie in collaborazione con tutte le amministrazioni statali interessate e con il contributo di personalità del mondo dell'università, della ricerca, dell'imprenditoria, degli ordini professionali e delle associazioni di categoria.

L'Italia è tra le prime nazioni a dotarsi di un simile strumento normativo, frutto di una rielaborazione in chiave moderna delle numerose leggi e norme che riguardano l'utilizzo delle tecnologie dell'informazione e della comunicazione da parte degli uffici pubblici nei rapporti con cittadini e imprese, sia la loro adozione nei rapporti giuridici tra privati. Il Codice dell'amministrazione digitale rappresenta una vera e propria "costituzione digitale" che in oltre settanta articoli definisce diritti e doveri, principi e prospettive del cittadino italiano nella Società dell'Informazione.

L'art. 2 (Finalità e ambito di applicazione) stabilisce, al primo comma che " Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione".

Il secondo comma prevede che "Le disposizioni del presente codice si applicano alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, salvo che sia diversamente stabilito, nel rispetto della loro

autonomia organizzativa e comunque nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione".

Nella Pubblica Amministrazione digitale i cittadini e le imprese hanno nuovi diritti che il Codice precisa e definisce e che rende quindi effettivamente esercitabili:

Diritto all'uso delle nuove tecnologie (art. 3)

I cittadini e le imprese hanno diritto di usare le moderne tecnologie informatiche per tutti i rapporti con qualsiasi amministrazione dello Stato. Non sarà più possibile quindi per un'amministrazione o per un gestore di pubblico servizio obbligare i cittadini a recarsi agli sportelli per presentare documenti cartacei, per firmare fisicamente domande o istanze, per fornire chiarimenti: per tutto questo deve essere sempre e dovunque disponibile un canale digitale sicuro, certificato e con piena validità giuridica che permetta di dialogare con la PA dal proprio computer.

Diritto all'accesso e all'invio di documenti digitali (art. 4)

In particolare i cittadini e le imprese hanno diritto di accedere a tutti gli atti che li riguardano e di partecipare a tutti i procedimenti in cui sono coinvolti tramite le moderne tecnologie informatiche e telematiche. Tutte le amministrazioni devono quindi organizzarsi per rendere disponibili agli interessati documenti, atti e procedimenti, in modo sicuro e trasparente, in formato digitale.

Diritto ad effettuare qualsiasi pagamento in forma digitale (art. 5)

Dal 1° gennaio 2006 i cittadini e le imprese avranno il diritto di effettuare in modo sicuro qualsiasi pagamento verso le pubbliche amministrazioni centrali attraverso le tecnologie informatiche e telematiche. Non sarà quindi più necessario alcun passaggio materiale di denaro né tanto meno fare file in banca o alla posta

Diritto a ricevere qualsiasi comunicazione pubblica per e-mail (art. 6)

I cittadini e le imprese che ne fanno richiesta hanno diritto a ricevere tutte le comunicazioni dalle pubbliche amministrazioni via e-mail all'indirizzo che avranno dichiarato. La posta elettronica proveniente dalla PA sarà certificata, ossia sarà certa la data e l'ora della spedizione, della sua ricezione e provenienza. Le comunicazioni e i documenti ricevuti in questo modo avranno piena validità giuridica anche verso altre persone o aziende.

Diritto alla qualità del servizio e alla misura della soddisfazione (art. 7)

I cittadini e le imprese hanno diritto a servizi pubblici di qualità e che rispondano

alle loro reali esigenze. Le pubbliche amministrazioni devono organizzare i servizi in modo da controllarne periodicamente la qualità e la soddisfazione dell'utenza.

Diritto alla partecipazione (art. 8)

I cittadini hanno diritto di partecipare al processo democratico e di esercitare i diritti politici usufruendo delle possibilità offerte dalle nuove tecnologie.

Diritto a trovare on-line tutti i moduli e i formulari validi e aggiornati (art. 58)

Entro due anni i cittadini e le imprese avranno diritto a trovare in rete tutti i moduli e i formulari e tutti i documenti rilevanti per qualsiasi pratica verso le pubbliche amministrazioni. I moduli, i formulari e i documenti che non fossero disponibili in via telematica non saranno più giudicati validi, o almeno non saranno più necessari.

Nella PA digitale questi diritti sono garantiti dalla disponibilità dei seguenti strumenti innovativi a cui il Codice dà piena validità giuridica:

La posta elettronica certificata (art. 6 e art. 51)

Si tratta di una e-mail che garantisce ora e data di spedizione e di ricezione, provenienza (con una firma elettronica) e integrità del contenuto. D'ora in poi vale quanto una raccomandata con ricevuta di ritorno, costituisce una prova certa, costa molto meno e si può fare da casa.

La firma digitale (art. 21)

È una firma elettronica che garantisce con sicurezza l'identificazione di chi firma e la sua volontà di firmare. Questa firma può sostituire per sempre sigilli, punzoni, timbri e dà validità giuridica a qualsiasi attestazione nei rapporti tra privati, tra privati e pubbliche amministrazioni e tra amministrazioni. Per rendere più sicura la firma elettronica questa deve essere certificata da un ente certificatore che risponda ai requisiti di legge e che si faccia garante dell'affidabilità della firma. Il codice regola tale certificazione in modo da conferire massima sicurezza alla firma elettronica, meglio di quanto ora avviene con la firma autografa.

I documenti informatici (art. 17 e segg.; art. 37; art. 42 e segg.; art. 46 e segg.)

Un documento informatico, sottoscritto con una firma elettronica certificata, ha sempre e dovunque la stessa identica validità del documento cartaceo ad ogni effetto di legge e deve essere accettato da qualsiasi soggetto pubblico o privato. È possibile quindi sostituire i documenti cartacei con documenti informatici, con considerevoli

vantaggi di tempo. Anche tutti i documenti contabili che la legge impone di conservare possono essere sostituiti da documenti informatici secondo le regole prescritte dal Codice e possono quindi essere conservati in forma digitale. Le pubbliche amministrazioni possono raccogliere tutti i documenti relativi ad un procedimento in un fascicolo elettronico e devono comunicare ai cittadini interessati come accedervi, secondo quanto prescrive la legge sulla trasparenza (L. 241/90).

Il Codice obbliga tutte le amministrazioni a gestire i documenti con sistemi informatici mediante il protocollo elettronico (certo e non modificabile, a garanzia di equità e di trasparenza, scoraggia malcostumi e forme di corruzione) e l'archiviazione elettronica che consente enormi risparmi di spazio e soprattutto di rintracciare velocemente qualsiasi documento tra i miliardi di documenti conservati dalle pubbliche amministrazioni.

I siti Internet della PA (artt. 56-57)

Quasi tutte le pubbliche amministrazioni hanno già i loro siti Internet, ma il codice ne rende obbligatorie alcune caratteristiche fondamentali: i siti pubblici devono essere accessibili da tutti, anche dai disabili, reperibili, facilmente usabili, chiari nel linguaggio, affidabili, semplici, omogenei tra loro.

I siti Internet diventano la "porta" privilegiata per entrare nelle pubbliche amministrazioni e sono tenuti quindi a riportare alcuni dati necessari per orientarsi: l'organigramma per sapere chi fa cosa; gli indirizzi e-mail a cui rivolgersi per ciascuna necessità; l'elenco dei servizi forniti in rete; l'elenco di tutti i bandi di gara; l'elenco dei procedimenti svolti da ciascun ufficio con la loro durata e il nome del responsabile. Dopo 15 anni la legge sulla trasparenza diventa quindi concreta. Non bisogna fare più domande per vedere lo stato di una pratica o sapere chi ne è il responsabile e quanto deve durare il procedimento: queste notizie devono essere già a disposizione sul sito della pubblica amministrazione interessata.

Le carte elettroniche (art. 67)

La carta di identità elettronica e la carta nazionale dei servizi diventano lo strumento chiave per razionalizzare e semplificare l'azione amministrativa e sono regolate dal Codice per essere uno strumento di autenticazione e di accesso ai servizi in rete della PA che sia universalmente valido in Italia, ma allo stesso tempo che

contenga quei servizi e quelle utilità che ciascuna amministrazione territoriale giudichi utile per i propri cittadini.

Nella PA digitale le amministrazioni cooperano tra loro e costituiscono una rete integrata di cui il Codice definisce principi e finalità:

Il federalismo efficiente (art. 12)

LA PA digitale, integrata e interconnessa in rete, è il fattore chiave per costruire un federalismo efficiente. A tal fine il Sistema Pubblico di Connettività costituisce lo strumento che consente ai soggetti pubblici di dialogare, scambiare dati e documenti attraverso standard condivisi e canali sicuri: una rete fatta dalle reti delle pubbliche amministrazioni, che mette in comunicazione PA centrale, PA locale, regioni e soggetti erogatori di servizi pubblici.

La cooperazione (art. 10 e art. 64)

Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e comunicazione garantendo l'accesso alla consultazione, la circolazione, lo scambio di dati e informazioni, l'interoperabilità, ossia la capacità dei sistemi informatici di scambiarsi e di usare mutuamente informazioni anche se diversi. Le pubbliche amministrazioni devono inoltre collaborare integrando i procedimenti di rispettiva competenza per rendere più efficienti i processi e agevolare i cittadini e le imprese nei loro adempimenti con la PA.

La riorganizzazione gestionale e dei servizi (art. 13)

Il Codice lega strettamente l'utilizzo delle tecnologie al raggiungimento di obiettivi di efficacia, efficienza, economicità dell'attività amministrativa. Le pubbliche amministrazioni devono utilizzare le tecnologie in modo da razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, la modulistica, le modalità di accesso ai servizi. Non basta informatizzare: l'innovazione tecnologica deve essere chiaramente orientata ad una maggiore efficienza interna ed efficacia dei servizi resi a cittadini e imprese.

La gestione informatica dei procedimenti (art. 37)

Con il Codice nasce il fascicolo informatico[1]*. Le pubbliche amministrazioni devono gestire i procedimenti utilizzando le nuove tecnologie e possono raccogliere in*

[1] Il Consiglio Regionale del Piemonte ha già varato l'esperienza di un "fascicolo digitale", con il dossier virtuale, strumento per l'informatizzazione dell'iter dei progetti di legge e delle deliberazioni consiliari: tutti i documenti che

un "fascicolo digitale" atti e documenti relativi ad un procedimento anche se prodotti da amministrazioni diverse. In questo modo si accelerano tempi e procedure interne, con maggiore efficienza, minori costi per la pubblica amministrazione e maggiore trasparenza per i cittadini.

La trasmissione informatica dei documenti (artt 50 e segg.)

Le amministrazioni possono comunicare e trasmettere documenti tra di loro in tempo reale. Il codice dà piena validità giuridica all'utilizzo della posta elettronica nella comunicazione tra uffici pubblici. Anzi è lo strumento con cui di norma le amministrazioni devono comunicare. Comunicazioni, atti e documenti trasmessi per e-mail tra uffici pubblici sono validi ai fini del procedimento amministrativo in tutti i casi in cui è possibile accertare la provenienza e cioè se sono siglate con la firma digitale, oppure con protocollo informatico o trasmessi con posta certificata.

La disponibilità dei dati (art. 53 e art. 60)

Le pubbliche amministrazioni devono rendere disponibili all'utilizzo da parte di altre amministrazioni i dati di cui sono in possesso, attraverso le tecnologie informatiche e telematiche. Ciascuna pubblica amministrazione titolare di dati è quindi tenuta a renderli accessibili, nell'ambito del Sistema Pubblico di Connettività, ad altri soggetti pubblici che ne fanno richiesta per lo svolgimento dei propri compiti istituzionali.

Le basi di dati di interesse nazionale (art. 62)

Il Codice individua come basi di dati di interesse nazionale un insieme di informazioni, omogenee per tipologia e contenuto, come ad esempio gli archivi delle anagrafi, che sebbene siano possedute da pubbliche amministrazioni diverse, sono necessarie ad altre pubbliche amministrazioni per lo svolgimento dei propri compiti. Le basi di dati di interesse nazionale costituiscono un sistema informativo unitario che deve essere gestito, nel rispetto delle competenze dell'amministrazione che possiede i dati, garantendo l'allineamento delle informazioni e l'accesso da parte delle amministrazioni interessate nell'ambito del Sistema Pubblico di Connettività. E' questa novità introdotta dal Codice che renderà possibile, ad esempio, passare dall'autocertificazione alla de-certificazione: eliminare cioè la richiesta di un gran numero di certificazioni da parte delle pubbliche amministrazioni

---

precedono, accompagnano e seguono l'esame e l'approvazione di questi atti da parte dell'Assemblea regionale sono consultabili on line (www.consiglioregionale.piemonte.it/dvpdlint/jsp/Start.jsp).

La PA digitale costa meno.

La pubblica amministrazione nel suo complesso già spende cifre considerevoli in nuove tecnologie (circa 1.300 milioni di euro la PA locale e circa 1.800 milioni di euro la PA centrale e gli Enti non economici) e ha dotato quasi tutti i dipendenti (91% dei posti "informatizzabili") di un posto di lavoro in rete, ma a tale sforzo spesso non si è accompagnato un incremento effettivo di efficienza e quindi un risparmio nei costi di funzionamento.

Il Codice mette le condizioni per realizzare una PA che sia più efficiente, elimini gli sprechi e in definitiva costi meno.

L'azzeramento dei certificati (art. 53)

Sono 35 milioni i certificati prodotti annualmente dalle pubbliche amministrazioni con un costo per i cittadini di circa 13,50 euro per ciascun certificato. La PA digitale potrà praticamente azzerare il numero dei certificati necessari attraverso la trasmissione dei documenti tra amministrazioni e la condivisone dei database. I cittadini e le imprese potrebbero quindi risparmiare oltre 400 milioni di euro.

L'uso della posta elettronica (artt. 6; 49; 50; 51; 52)

Si sono stimati in 31 milioni i messaggi di posta elettronica inviati tra pubbliche amministrazioni e nei contatti di queste con l'esterno e in 18 euro il risparmio ottenuto per messaggio rispetto alla gestione di un messaggio di posta fisico. Il Codice, riconoscendo piena validità giuridica alle comunicazioni per via telematica, pone le basi per un incremento di tale numero e soprattutto per una sostituzione quasi totale della vecchia trasmissione cartacea. Una stima prudente valuta in circa 360 milioni di euro i risparmi che ne potrebbero derivare già dal prossimo anno.

Gli archivi digitali (artt. 46 e segg.)

Con il Codice la pubblica amministrazione senza carta diventa realtà. Tutti gli atti, i dati, i documenti, le scritture contabili ed anche la corrispondenza prodotti o riprodotti in maniera digitale secondo le regole che garantiscono la conformità agli originali hanno la stessa validità giuridica di documenti cartacei e devono essere conservati in archivi informatici. Grazie alla conservazione digitale, si riducono tempi e costi di ricerca dei documenti, ma anche i costi di gestione e manutenzione degli

archivi: processi più veloci, risparmi di spesa per le amministrazioni, enorme recupero di spazi prima occupati da ingombranti archivi cartacei.

Le conferenze dei servizi on-line (art. 37)

Quando un qualsiasi procedimento pubblico (una licenza, una nuova opera pubblica, un evento, ecc.) coinvolge più amministrazioni, per semplificare il suo svolgimento viene indetta una "conferenza dei servizi" a cui partecipano responsabili di tutti gli enti interessati. Ora il Codice prevede la possibilità che queste conferenze si svolgano on-line, evitando viaggi, spese di trasferta, perdite di tempo e quindi con un notevole risparmio di denaro e una maggiore velocità.

Il riuso delle tecnologie (artt. 70 e segg.)

Il Codice istituisce la banca dati dei programmi informatici riutilizzabili, un elenco di programmi applicativi di proprietà pubblica. Prima di acquisire nuove applicazioni tecnologiche le pubbliche amministrazioni devono verificare se vi sono soluzioni riutilizzabili, che sono cedute in maniera gratuita dalle amministrazioni titolari. Il processo di riuso abbatte i costi degli investimenti in tecnologie e aiuta anche le amministrazioni con minore capacità di spesa ad acquisire tecnologie innovative. In questo modo tutte le amministrazioni, dalle più grandi alle più piccole potranno erogare servizi avanzati a cittadini e imprese.

Gli sportelli per le imprese (art. 9)

Gli sportelli unici per le attività produttive diventano telematici: devono riorganizzarsi per gestire i procedimenti e le attività interne in maniera informatica, acquisire istanze da parte delle imprese ed erogare i servizi attraverso internet e posta elettronica. Per ottenere una maggiore efficienza e per risparmiare risorse il Codice prescrive forme di coordinamento tra le varie amministrazioni interessate che permetterà alle imprese di trovare ovunque una procedura omogenea. A livello centrale nasce il registro informatico degli adempimenti amministrativi di competenza delle amministrazioni centrali, nell'ambito però di una rete integrata di servizi gestiti dagli sportelli sul territorio.

E' infine doveroso sottolineare che in dottrina non mancano appunti a talune disposizioni del codice e che molti di questi rilievi si avvalgono del parere, in conclusione favorevole ma particolarmente critico, del Consiglio di Stato 7 febbraio

11995/2005, riportato nella scheda n. 5976, parere del quale il legislatore ha tenuto poco conto nella redazione del testo finale del decreto.

Si contesta, da parte di alcuni autori, la stessa natura di testo unico del Codice dell'amministrazione digitale: viene infatti rilevato che testi importanti, quali in particolare il d.p.r. n. 68/2005 (in materia di posta elettronica certificata) ed il d.lgs. n. 42/2005 (che istituisce il Sistema Pubblico di Connettività) non sono entrati a fare parte del testo del

Codice.

Si segnala, inoltre, il parere del Consiglio di Stato (Sezione Consultiva per gli Atti Normativi) n. 31/2006 con il quale il Consiglio di Stato, pronunciandosi sullo schema di decreto legislativo recante disposizioni correttive e integrative al decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale), fa un discorso generale dal quale si evince che, "pur in presenza di un panorama normativo di avanguardia nella materia dell'informatica pubblica, sono mancate, nel corso di questi anni, quelle azioni collaterali - ma evidentemente essenziali - che fanno si che un complesso di disposizioni così innovativo e di così ampio respiro sia effettivamente e concretamente attuato.

Pubblicate in GU le Linee guida per la PA digitale

NUMERO SCHEDA: 6980

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: CODICE DELLA AMMINISTRAZIONE DIGITALE

FONTE: CNIPA

RIFERIMENTO NORMATIVO: d.lgs. n. 82/2005

NATURA ATTO: DIRETTIVA

SCHEDE COLLEGATE: 6230

Sulla Gazzetta Ufficiale numero 16 del 20 gennaio 2006 è stata pubblicata la Direttiva del 18 novembre 2005 del Dipartimento per l'Innovazione e le Tecnologie "Linee guida per la Pubblica amministrazione digitale" che fissa i criteri e le azioni che tutte le pubbliche amministrazioni dovranno attuare per realizzare concretamente i principi contenuti nel Codice dell'Amministrazione digitale.
La 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.
Il Codice, entrato in vigore il 1º gennaio 2006, contiene le disposizioni per garantire il diritto di ogni cittadino a usufruire dei servizi della P.A. anche on line e l'obbligo per la P.A. di snellire le procedure ed e rendere tutti i servizi e le comunicazioni interne ed esterne per via telematica.
La 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 PA gli strumenti tecnico-giuridici attraverso cui ripensare la propria organizzazione in chiave digitale per fornire a cittadini ed imprese i propri servizi on line con una progressiva riduzione dei costi ed un incremento dell' efficienza e della trasparenza.
La direttiva si compone delle seguente parti:

- premessa;
- 1) Comunicazione telematica tra pubblica amministrazione e cittadini;
- 2) Comunicazione interna alle pubbliche amministrazioni;
- 3) Carta Nazionale dei Servizi;
- 4) Transazioni economiche on line;
- 5) Conferenza di servizi on line;
- 6) Sicurezza dei sistemi informativi;
- 7) Strutture per l'organizzazione, l'innovazione e le tecnologie.

In particolare la direttiva, invita le P.A.

- - a consentire ai cittadini titolari delle Carte Nazionali dei Servizi (CNS) l'accesso ai servizi pubblici, indipendentemente dall'ente di emissione delle stesse fornendone un'informazione adeguata;
- - a consentire i pagamenti on line;
- - a garantire riservatezza e integrità dei contenuti, continuità e disponibilità dei servizi mettendo in pratica le disposizioni contenute nella direttiva sulla sicurezza informatica e delle telecomunicazioni del 16 gennaio 2002

- - a individuare un centro di competenza interno a ciascuna P.A. cui afferiscano, tra l'altro, compiti di coordinamento strategico dello sviluppo dei sistemi informativi.

Si allega il testo della direttiva.

PRESIDENZA DEL CONSIGLIO DEI MINISTRI - DIPARTIMENTO PER L'INNOVAZIONE E LE TECNOLOGIE - DIRETTIVA 18 novembre 2005 (in *G.U.* n. 16 del 20 gennaio 2006) - Linee guida per la Pubblica amministrazione digitale.

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 connettivita» 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, allorchè 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.

Un interessante commento sulle novità del cosiddetto decreto competitività in tema di innovazione tecnologica e sui rapporti con il codice dell'amministrazione digitale.

NUMERO SCHEDA: 6624

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: CODICE DELLA AMMINISTRAZIONE DIGITALE

FONTE: DIRITTO E GIUSTIZIA

AUTORE: Michele Iaselli

NUMERO: 26

DATA: 02/07/2005

PAGINA: 103-105

RIFERIMENTO NORMATIVO: d.l. n. 35/2005; l.n. 80/2005

NATURA ATTO: COMMENTO

SCHEDE COLLEGATE: 6072; 6225

Sulla rivista "D&G Diritto e Giustizia", n. 26/2005, è pubblicato un interessante articolo di Michele Iaselli, intitolato "*L'ente diventa efficiente: via al digitale. E-mail certificate, banda larga e annotazioni on line al Pra*".

Il commento, partendo dall'analisi delle novità che, in materia di innovazione tecnologica, ha previsto il cosiddetto decreto competitività (decreto legge n. 3572005, convertito con modifiche in legge n. 80/2005; v. scheda n. 6072 e scheda n. 6225),

analizza le disposizioni del decreto, soprattutto quelle inerenti la semplificazione amministrativa, in rapporto ad alcune importante disposizioni contenute nel codice dell'amministrazione digitale.
L'articolo, che è in visione presso il settore Studi e documentazione legislativi, dopo una breve premessa, si suddivide nelle seguenti parti:
- Gli obiettivi.
- Le novità del decreto.
- Il nodo della trasmissione.

Un interessante articolo sull'evoluzione della disciplina del documento informatico.

NUMERO SCHEDA: 6600

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: CODICE DELLA AMMINISTRAZIONE DIGITALE

FONTE: RIVISTA DI DIRITTO CIVILE

AUTORE: Francesco Delfini

NUMERO: 3

DATA: 30/09/2005

PAGINA: 531-542

NATURA ATTO: COMMENTO

NUM. ATTO: 2005

Sul numero 3/2005 della "Rivista di diritto privato" è pubblicato un interessante articolo, a cura di Francesco Delfini, intitolato "L'evoluzione normativa della disciplina del documento informatico: dal d.p.r. 513/1997 al Codice dell'amministrazione digitale".
Si riporta il sommario del commento, che è consultabile presso il settore Studi e documentazione legislativi.

1. Il Codice dell'amministrazione digitale e la sua applicabilità ai privati.
2. L'impianto originario: il d.p.r. 513/1997.
3. Il Testo Unico sulla Documentazione Amministrativa (TUDA) di cui al d.p.r. 445/2000.
4. Le modifiche del TUDA per effetto del recepimento, con il d.lgs. 10/2002, della direttiva 1999/93/CE in tema di firme elettroniche.
5. Le ulteriori modifiche in punto di firme elettroniche introdotte dal d.p.r. 137/2003.
6. La disciplina del documento informatico nel d.lgs. 82/2005.

Il codice dell'amministrazione digitale conferisce un nuovo rilievo alle informazioni pubbliche che possono essere rese disponibili in modalità

digitale e quindi più celermente e ad un numero di cittadini sempre maggiore.

NUMERO SCHEDA: 6293

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: CODICE DELLA AMMINISTRAZIONE DIGITALE

FONTE: INTERLEX

NATURA ATTO: COMMENTO

DATA ATTO: 10/01/2005

SCHEDE COLLEGATE: *6230* *6306*

Il commento qui di seguito allegato pone l'accento sulla rilevanza di alcuni articoli del codice dell'amministrazione digitale: l'articolo 56, ad esempio, permette al cittadino di conoscere l'attività della pubblica amministrazione indipendentemente dalla disciplina relativa all'accesso agli atti del procedimento amministrativo anche se, i medesimi, reperibili con modalità digitali, finiscono per modificare il valore stesso del procedimento amministrativo.
Inoltre, dall'analisi delle disposizioni del codice, si evince chiaramente che la tendenza è quella di rendere accessibile il maggior numero di documenti e, attraverso i siti web pubblici, di fornire il più celermente possibile tutte le informazioni utili al cittadino, in un'ottica di trasparenza ed efficienza della p.a.
L'articolo57, per garantire la sicurezza dei dati stabilisce anche i contenuti obbligatori dei siti pubblici e, in particolare, prevede che le informazioni raccolte in tali siti dovranno corrispondere a quelle contenute nei procedimenti amministrativi di cui si fornisce comunicazione.

Si allega il commento.

Gli strumenti di interazione tra amministrazioni e privati. Siti web pubblici e posta elettronica certificata

Lo schema del codice affronta la questione relativa agli strumenti di dialogo tra cittadino e PA, e individua da un lato le reti telematiche (art. 10, comma 4) ed i siti web pubblici (artt. 56 e 57) per la disponibilità di dati ed informazioni digitali e per la fornitura di servizi in rete, dall'altro lato la posta elettronica certificata (art. 6) per lo scambio di atti e documenti amministrativi informatici.
Quanto alle reti telematiche, la dichiarazione di principio contenuta all'art. 10, c. 4 – come già detto nel primo articolo di questa serie, certamente al di fuori dei limiti tracciati dalla legge delega – è, nella sostanza, inequivocabile: "La Repubblica promuove la realizzazione e l'utilizzo di reti telematiche come strumento di interazione tra le pubbliche amministrazioni ed i privati". Per quanto concerne i siti web pubblici, il codice statuisce altrettanto chiaramente che "le pubbliche amministrazioni centrali realizzano siti istituzionali su reti telematiche che rispettano i principi di usabilità, reperibilità, accessibilità anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità ed interoperabilità" (art. 56, comma 1).
La rilevanza di queste disposizioni è notevole, in considerazione del fatto che la attività amministrativa non ruota più soltanto intorno al documento amministrativo, ma anche al dato ed alla informazione che amministrazioni statali, regionali ed enti locali, grazie alla telematica, possono rendere disponibili direttamente nelle case dei cittadini. I dati informatici viaggeranno attraverso le reti telematiche e

verranno infine pubblicati e resi conoscibili sui siti Internet delle PA al tempo stesso bacheche e sportelli virtuali. Il decreto in esame pare recepire e codificare queste tendenze evolutive del procedimento amministrativo, sancendo la nuova rilevanza che in esso assume l'informazione in modalità digitale (art. 2, comma 1).
In concreto, al fine dell'implementazione delle reti telematiche pubbliche, è stato approvato in via preliminare dal CdM e dalla Conferenza unificata stato-regioni-autonomie locali, lo schema di DLgs recante "Istituzione del sistema pubblico di connettività", norma intimamente connessa al codice in commento, in quanto prevede e disciplina le infrastrutture tecnologiche su cui "gireranno" le regole e gli strumenti procedimentali messi a punto dal codice dell'amministrazione digitale (vedi E. De Giovanni, Pubblica Amministrazione e ICT: le iniziative del Ministro per l'Innovazione e le Tecnologie, su Telejus).
Quanto ai siti web pubblici, il codice, dopo essersi preoccupato della loro uniformità e standardizzazione, promuovendo intese ed azioni comuni tra Stato, regioni e enti locali (art. 56, comma 2), dedica un intero articolo – l'art. 57 – ai dati pubblici che dovranno necessariamente contenere.
Da notare, innanzitutto, le prescrizioni relative all'elenco delle caselle di posta elettronica istituzionali attive, anche se non di posta elettronica certificata, l'elenco di tutti i bandi di gara e quello dei servizi forniti in rete.
Inoltre, vi sono alcune prescrizioni più specificamente relative al procedimento amministrativo, che non sono altro che la versione "virtuale" delle disposizioni previste dalla legge 7 agosto 1990, n. 241 e quindi già vincolanti per la PA nella sua attività in forma cartacea, tanto che il codice si preoccupa di chiarire che tali informazioni contenute nei siti Web pubblici dovranno essere conformi e corrispondenti a quelle contenute nei provvedimenti amministrativi originali dei quali si fornisce comunicazione tramite il sito (art. 57, comma 4): tali informazioni sono l'elenco dei procedimenti svolti, i termini previsti per la loro definizione, le unità organizzativa responsabili di istruttoria, dell'adozione del provvedimento finale, nonché il responsabile del procedimento.
Da segnalare, infine, le prescrizioni secondo cui i siti delle pubbliche amministrazioni centrali dovrebbero necessariamente contenere anche l'organigramma, l'articolazione degli uffici, le attribuzioni e l'organizzazione di ciascun ufficio, nonché il settore dell'ordinamento giuridico riferibile all'attività da essi svolta, con documenti anche normativi di riferimento: si impongono così alle PA nuovi oneri di comunicazione non altrimenti previsti da precedenti norme.
Passando alla posta elettronica certificata, essa nel testo in esame assurge a "strada virtuale maestra" per ogni scambio di documenti nella attività esterna delle amministrazioni centrali.
E ciò trova conferma nel fatto che, tra le definizioni cristallizzate all'art. 1, ve ne è una completamente nuova, non precedentemente prevista dal Dpr 445/2000, secondo cui è "indirizzo elettronico" una casella di posta elettronica idonea ad identificare una struttura tecnologica in grado di trasmettere, ricevere e mantenere a disposizione messaggi di posta elettronica. Tale ruolo preminente è peraltro confermato dal carattere chiaramente programmatico dell'art. 6: "Le pubbliche amministrazioni centrali utilizzano la posta elettronica certificata… per ogni scambio di documenti e informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata".
La suddetta norma fa riferimento specifico proprio al decreto del Presidente della Repubblica recante Disposizioni per l'utilizzo della posta elettronica certificata, approvato dal Consiglio dei ministri il 25 marzo 2004 e, da ultimo, accolto con parere favorevole dalla 1^ Commissione affari costituzionali del Senato il 13 ottobre scorso, ma non ancora entrato in vigore. Il codice, pertanto, riconosce oggi alla PEC quella primaria importanza che già era stata riconosciuta la scorsa primavera nell'ambito del processo di digitalizzazione della PA (vedi C. Giurdanella ed E. Guarnaccia, La posta elettronica certificata: conferma normativa per la P.A., innovazione per i privati, su Altalex). Ulteriore conferma del primario ruolo che la posta certificata avrà nella nuova amministrazione informatizzata è data dal recente decreto del Ministero della giustizia n. 272 del 14 ottobre 2004, contenente le regole tecniche del processo civile telematico (per un primo commento, vedi C. Giurdanella, Depositi «elettronici» al Tar Catania: spunti per un processo amministrativo telematico, su Giustizia Amministrativa).
Ed infatti, il capo II, rubricato "Gestione della posta elettronica certificata", individua la PEC come unico strumento di dialogo per tutti i soggetti coinvolti nel processo telematico. Ognuno dovrà disporre di un unico indirizzo elettronico da utilizzare nel processo, e della relativa casella di posta elettronica, la cosiddetta CPECPT (art. 11, comma 2). Tale indirizzo sarà, peraltro, abilitato a ricevere esclusivamente messaggi provenienti da indirizzi elettronici del medesimo sistema (commi 3 e 4).
Per quanto concerne il codice in commento, oltre al limite relativo all'uso facoltativo nelle attività interne della PA, già sancito dal suddetto schema di DPR, il secondo comma dell'art. 6 introduce la facoltatività anche per le pubbliche amministrazioni regionali e locali. Malgrado ciò, questa disposizione

ci pare, non solo da un punto di vista sistematico, una previsione chiave del nuovo sistema, punto di congiunzione tra riorganizzazione strutturale e gestionale. Da un lato, infatti, la posta certificata sembra essere il canale telematico di comunicazione a cui il legislatore si affida maggiormente, e per questo ne viene prevista genericamente la sua adozione nel capo I del codice; dall'altro essa, quale strumento gestionale di dialogo della PA, diventa lo strumento di trasmissione all'interno dei procedimenti amministrativi, e per questo viene ripreso nel capo III, che ne descrive modalità di utilizzo ed effetti giuridici connessi.
D'altronde, ad una breve analisi delle norme relative al sistema di gestione informatica dei documenti, le uniche modifiche - peraltro di notevole rilievo – che il codice apporta al disposto normativo già previsto dal TU sulla documentazione amministrativa, sono proprio quelle relative alla trasmissione informatica dei documenti e ad i suoi strumenti. Analizziamole brevemente.
Lo strumento attorno a cui ruoterà, ai sensi del nuovo codice, la trasmissione informatica dei documenti è proprio la posta elettronica certificata, sia tra le pubbliche amministrazioni (art. 50, c. 1 e 2), che per tutte le comunicazioni con l'esterno che necessitano di una ricevuta di invio ed una di consegna (art. 51).
Solo per le comunicazioni tra l'amministrazione ed i propri dipendenti è sufficiente, ma necessaria, la normale posta elettronica (art. 50, co. 3, lett. b). Quanto alle comunicazioni tra le pubbliche amministrazioni, è richiesto l'utilizzo della posta elettronica purché se ne verifichi la provenienza. Ora, ai sensi dell'art. 50, comma 2, ai fini della verifica della provenienza, le comunicazioni sono valide solo se sottoscritte con firma digitale o se trasmesse attraverso sistemi di posta elettronica certificata, previsione che, di fatto, per ragioni pratiche ed economiche, finirà per trovare applicazione solo con l'utilizzo di sistemi di posta elettronica certificata.
Si assiste, peraltro, ad una radicale modifica del vecchio art. 14, DPR 445/2000. Innanzi tutto, trasfuso nell'art. 51 del codice, esso non è più rubricato "trasmissione del documento informatico", ma "posta elettronica certificata". Ad esso, inoltre, viene aggiunto un comma, che così inequivocabilmente statuisce: "la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata". Tale specifica modalità di trasmissione viene quindi legata alla vecchia equiparazione alla notificazione per mezzo della posta, che il TU legava invece a più generiche modalità di trasmissione del documento informatico che avrebbero dovuto assicurarne la consegna (art. 14, c. 3, DPR 445/2000).
Viene, inoltre, inequivocabilmente palesata la volontà di dare rilevanza giuridica a queste due fasi del "viaggio telematico" della posta elettronica (invio e consegna): il documento informatico trasmesso per via telematica si intende inviato dal mittente se trasmesso, e si intende consegnato al destinatario, se disponibile all'indirizzo elettronico da questi dichiarato (art. 49, c. 1). il Codice, dunque, modifica anche il primo comma dell'art. 14, DPR 445/2000, e lo fa così come era già stato proposto di fare con lo schema di decreto sulla posta elettronica certificata: non più un'unica presunzione (di conoscibilità) che si forma quando il messaggio è trasmesso all'indirizzo elettronico dichiarato dal destinatario, ma due presunzioni (di invio e di consegna) che si formano rispettivamente quando il messaggio elettronico viene trasmesso, e quando risulta disponibile all'indirizzo elettronico del destinatario.
Tuttavia, questa inequivocabile presa di posizione del DIT, corroborata dal Ministero della giustizia, oggi non può che rimanere tale, essendo ancora lontana dall'essere una disciplina, giuridica e tecnica, di immediata ed effettiva applicazione. E ciò trova conferma proprio nelle suddette osservazioni formulate lo scorso 13 ottobre dal Senato sullo schema di DPR sulla posta elettronica certificata. Ed infatti, genericità ed astrattezza del suddetto DPR sono evidenziate dalla pragmaticità di alcune indicazioni parlamentari, tra le quali, in particolare, la necessità di chiarire le modalità con cui ogni cittadino debba rendersi disponibile all'utilizzo della posta elettronica certificata, se tale disponibilità debba darsi una volta per tutte o procedimento per procedimento, in che modo e a quali condizioni sarà possibile cambiare l'indirizzo di posta elettronica, quali saranno gli obblighi dei fornitori del servizio in ordine a disfunzioni, virus informatici o guasti.
Si tratta di problemi basilari, che il Governo, in particolare il Ministro per l'innovazione, a seguito della formale presa di posizione del Senato, non potrà non tenere in considerazione.

Lo Stato, ex art. 14 del codice dell'amministrazione digitale, disciplina il coordinamento dei dati dell'amministrazione statale, regionale e locale.

NUMERO SCHEDA: 6292

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: CODICE DELLA AMMINISTRAZIONE DIGITALE

FONTE: INTERLEX

NATURA ATTO: COMMENTO

L'articolo qui di seguito allegato, affronta brevemente la problematica relativa al coordinemanto informaticco fra Stato e regioni alla luce delle nuove disposizioni introdotte dal Codice dell'amministrazione digitale.
Il codice dedica un'intera sezione (Sez. III) del capo I alla disciplina dei rapporti fra le diverse amministrazioni, centrali e locali, prendendo anche posizione sulla ripartizione delle competenze legislative in materia informatica.
Il problema dei limiti del coordinamento informatico, di competenza statale, affrontato di recente dalla Corte Costituzionale in due distinte sentenze(1) pare risolto dal codice dell'amministrazione digitale agli articoli 12 e 14. Quest'ultimo articolo al comma1 precisa che :"In attuazione del disposto dell'articolo 117, secondo comma,lettera r), della Costituzione, lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilita' dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime".
Il coordinamento è anche assicurato da intese e accordi stipulati fra Stato, regioni e autonomie locali e dall' adozione, attraverso la Conferenza unificata, degli indirizzi utili per realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso e, infine dall'individuazione delle regole tecniche comuni.
Lo Stato inoltre istituisce organismi di cooperazione con le regioni e le autonomie locali, promuove intese ed accordi tematici e territoriali, favorisce la collaborazione interregionale, incentiva la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle
soluzioni tecniche ed organizzative, previene il divario tecnologico tra amministrazioni di diversa dimensione e collocazione territoriale.
(1) Corte Costituzionale, 16 gennaio 2004, n.17;Corte Costituzionale, 21 ottobre 2004, n.307.

Si allega il commento.

L' innovazione strutturale e il problema del coordinamento informatico stato-regioni.
Lo schema di codice dell'amministrazione digitale oggi approda alla Conferenza stato-regioni e quindi passerà al Consiglio di Stato, prima dell'esame da parte delle commissioni parlamentari. Continuando questa prima analisi del testo, pare utile soffermarci su quelle disposizioni con cui il Dipartimento per innovazione e le tecnologie ha voluto porre le basi per una solida "ricostruzione digitale" della cosa pubblica.
In effetti, l'art. 13 pone in particolare rilievo la riorganizzazione strutturale (la digitalizzazione vera e propria), e la affianca, sullo stesso livello strategico e funzionale, alla riorganizzazione gestionale (il procedimento amministrativo elettronico, di cui si dirà nel prossimo numero).
Pare significativo, peraltro, che proprio in questa sezione III del capo I, il codice prenda posizione sul problema della ripartizione di competenze legislative in materia informatica tra Stato, regioni ed enti locali.

Per quanto riguarda più specificamente gli strumenti tecnici, il codice dell'amministrazione digitale prende avvio proprio da dove si era fermato il legislatore con il testo unico sulla documentazione amministrativa (firma digitale, protocollo informatico, sistemi di gestione informatica dei documenti), ma lo fa ancora una volta in maniera più consapevole, in un'ottica di programmazione e sistematizzazione. Infatti, alcune delle norme di principio contenute nel capo I, sono specificamente dedicate proprio alle infrastrutture digitali della PA.
Inoltre digitalizzazione strutturale non significa solo "reingegnerizzazione dei procedimenti". Essa non può riguardare solo le cose, ma anche, e soprattutto, le risorse umane. Accanto alle strutture, va dunque rinnovata la cultura informatica, anche per mezzo di lunghi e non agevoli percorsi di alfabetizzazione all'interno delle amministrazioni. Ed ecco l'obbligo per le PA di prevedere, nell'ambito delle attività di gestione delle risorse umane e di predisposizione dei piani formativi ex art. 7-bis, D.Lgs 165/2001, precise politiche di formazione informatica del personale (art. 11).
Altre previsioni programmatiche risultano in questa sede degne di nota per la loro valenza sociale e democratica: i pagamenti con modalità informatiche (art. 5), e la partecipazione democratica elettronica (art. 8), che lo Stato deve incentivare, favorendo ogni forma di uso delle nuove tecnologie per una maggiore partecipazione dei cittadini al processo democratico e all'esercizio dei diritti politici e civili.
Ma veniamo a quello che, nella stesura attuale, a nostro avviso costituisce uno dei punti deboli del codice: il coordinamento informatico.
Il codice lo prevede innanzi tutto verso l'alto: la digitalizzazione, afferma il comma 3 dell'art. 10, deve essere operata garantendo comunque la partecipazione dell'Italia alla costruzione di reti transeuropee per lo scambio fra le amministrazioni dei Paesi della Unione europea. E fin qui nulla quaestio.
Luci ed ombre, invece, sul problema del coordinamento informatico interno, tra Stato e regioni, questione di particolare rilevanza perché attinente alla recente riforma del Titolo V della Costituzione ed alle sue concrete ricadute. Il codice, ad una prima veloce lettura, sembrerebbe discostarsi dalle posizioni recentemente adottate dalla giurisprudenza costituzionale, che per la verità si è occupata del problema solo due volte, con le sentenze del 16 gennaio 2004 n. 17, e del 21 ottobre 2004 n. 307. Il codice, infatti, opera all'art. 12 una interpretazione che sembrerebbe più restrittiva, da alcuni letta come non conforme ai suddetti pronunciamenti costituzionali, attribuendo allo Stato il compito di dettare solo le norme necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici, al precipuo fine di una completa ed efficiente circolazione e scambio dei dati, nonché il compito di favorire intese e accordi con le regioni e gli enti locali utili per realizzare "un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso".
Ma ad una breve analisi delle due citate sentenze ci si accorge che l'art. 12, in verità, non fa altro che allinearsi ad esse.
Con la prima decisione, la 17/2004, la Consulta si è espressa sul ricorso che le Regioni Marche, Toscana e Basilicata avevano proposto in via principale avverso l'art. 29, comma 7, lett. a) della legge 448/2001, il quale prevede che il Ministro per l'innovazione e le tecnologie, al fine di migliorare la qualità dei servizi e la razionalizzazione della spesa per informatica, debba definire indirizzi per l'impiego ottimale dell'informatizzazione nelle pubbliche amministrazioni, sentita la conferenza unificata Stato-Regioni-Città-Autonomie. La Corte decideva per la infondatezza di tale questione di legittimità costituzionale, con riferimento agli artt. 3, 5, 114, ed in particolare, al controverso art. 117 Cost., in quanto, secondo i giudici, il potere di coordinamento attribuito al ministro per l'innnovazione è di natura meramente tecnica, atto ad assicurare una comunanza di linguaggi, di procedure e di standard omogenei, e quindi a garantire la piena cooperazione operativa fra tutti i soggetti pubblici operanti sul territorio nazionale.
In altri termini, lo Stato può - rectius: potrebbe - solo dettare le regole tecniche e gli standard tecnologici necessari a garantire gli scambi di informazioni tra le varie amministrazioni, ma per ogni altra questione informatica (ad esempio, modelli operativi e gestionali e scelta dei vari software) vige la potestà legislativa ed organizzativa residuale delle regioni.
Non si discosta troppo da queste conclusioni la sentenza 307/2004. La Regione Emilia-Romagna denunciava l'incostituzionalità delle norme statali istitutive di fondi speciali destinati ad incentivare l'acquisto di personal computer da parte di giovani o di soggetti aventi determinati requisiti reddituali, mediante l'erogazione di contributi economici (progetti "PC ai giovani" e "PC alle famiglie"). La Corte decideva anche questa volta per il rigetto del ricorso regionale, affermando che lo Stato può prevedere incentivi all'uso del computer senza invadere la sfera di competenza delle regioni: "lo sviluppo della cultura, anche attraverso l'uso dello strumento informatico, è previsto dall'art. 9 della Costituzione, e prescinde dal riparto di competenze Stato-Regioni di cui all'art. 117 Cost.". Ancora una volta una larga interpretazione della espressione "coordinamento informatico", che sembra riconoscere allo Stato ampi spazi di movimento.

Ora, a ben vedere, lo schema di decreto governativo non ha fatto altro che "riempire" di significato la lett. r), dell'art. 117, comma 2, e lo ha fatto proprio ispirandosi a le due suddette decisioni. Desta qualche perplessità il fatto che la lettera della norma, così come astrattamente prevista, affermi un potere statale di coordinamento informatico "debole", di natura meramente tecnica, quando la Corte costituzionale, partendo dalla stessa posizione astratta – di fatto rifluita coscientemente nello schema del codice - ha già, in sostanza, respinto due ricorsi regionali in materia, riconoscendo indirettamente un importante potere di coordinamento centralizzato.
Tale potere "forte", peraltro, appare pure giustificabile per più considerazioni. Da un lato, i criteri tecnico-informatici sovente finiscono con diventare veri e propri standard, a cui vengono di conseguenza sottese inevitabili scelte di natura politica e, più in generale, ideologica, tutt'altro che tecnica. Si pensi, in particolare allo "scontro" dogmatico tra i fautori dell'open source e quelli del software proprietario (vedi, sul punto D. Marongiu, "Spunti di riflessione sul coordinamento dell'informatica pubblica", su Telejus).
Da altro punto di vista, la possibilità di ingerire nelle strutture organizzative degli enti, e di prevedere anche per esse l'adozione di determinati moduli organizzativi o di determinate piattaforme tecnologiche, potrebbe essere anche auspicabile in ossequio al principio di buona amministrazione sancito dall'art. 97 Cost.
Peraltro, alcune ingerenze statali possono comunque essere considerate legittime in ossequio ad altri principi costituzionali, non riconducibili all'art. 117 Cost., come è già accaduto nell'ipotesi affrontata dalla Corte costituzionale con sentenza 307/2004, che ha tutelato le scelte governative richiamando lo "sviluppo della cultura", fissato dall'art. 9, perseguibile anche attraverso l'uso dello strumento informatico. E ciò proprio per la loro natura, spesso politica.
Concludendo, pare evidente come questa disposizione codicistica nulla aggiunga ai dati normativi e giurisprudenziali che avevamo già, e nulla chiarisce in ordine all'interpretazione di quella lettera r), che pure è di enorme importanza per lo sviluppo "dialogato" dell'attività amministrativa informatizzata.
E', tuttavia, altrettanto evidente, come si è avuto già modo di dire nel commento della settimana scorsa, che, anche alla luce dell'appena commentato art. 12 del Codice, non tarderanno a presentarsi ai giudici costituzionali le occasioni per affrontare e dirimere una volta per tutte la questione.
* Avvocati, studio legale Giurdanella, Catania

Pubblicato sulla Gazzetta Ufficiale il codice dell'amministrazione digitale

NUMERO SCHEDA: 6230

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: CODICE DELLA AMMINISTRAZIONE DIGITALE

FONTE: GAZZETTA UFFICIALE

NUMERO: 112

DATA: 16/05/2005

NATURA ATTO: DECRETO LEGISLATIVO

DATA ATTO: 07/03/2005

NUM. ATTO: 82

SCHEDE COLLEGATE: 6042 6219 6292 6293 6306

Sul supplemento ordinario n. 93 alla Gazzetta Ufficiale n. 112 del 16 maggio 2005 è stato pubblicato il decreto legislativo n. 82 del 7 marzo 2005 "Codice dell'amministrazione digitale".

Si tratta di uno strumento che, come ha dichiarato il ministro dell'Innovazione Stanca, obbliga tutte le pubbliche amministrazioni, a partire dal 1 gennaio 2006, a fare ricorso all'informatica e ad accettarla come principale strumento operativo non solo nei rapporti interni, ma, soprattutto, in quelli con la collettività.
Per tutte le novità introdotte dal codice si rinvia alla scheda n. 6042.

Approvato dal Consiglio dei ministri in via definitiva il Codice dell'amministrazione digitale.

NUMERO SCHEDA: 6042

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: CODICE DELLA AMMINISTRAZIONE DIGITALE

FONTE: ITALIA OGGI

DATA: 05/03/2005

PAGINA: 21

NATURA ATTO: decreto legislativo

DATA ATTO: 07/03/2005

NUM. ATTO: 82

SCHEDE COLLEGATE: 6219 6230 6306

Nella seduta del Consiglio dei Ministri n. 197 del 4 marzo 2005 è stato approvato in via definitiva il decreto legislativo (d.lgs. 7 marzo 2005, n. 82, pubblicato sulla Gazzetta Ufficiale n. 112 del 16 maggio 2005, supplemento ordinario n. 93) che accorpa e riordina nel Codice dell'amministrazione digitale la normativa in materia di attività digitale delle pubbliche amministrazioni. Il Consiglio dei Ministri aveva già approvato in via preliminare nella riunione dell'11 novembre 2004 lo schema di decreto contenente tutte le norme sinora emanate per favorire la diffusione delle nuove tecnologie e l'ammodernamento delle p.a..
Il Codice tratta in modo organico il tema dell'utilizzo delle tecnologie dell'informazione e della comunicazione nelle strutture pubbliche, disciplinando i principi giuridici fondamentali relativi al documento informatico ed alla firma digitale.
Sullo schema di Codice sono stati acquisiti i pareri della Conferenza unificata, del Consiglio di Stato, delle Commissioni parlamentari competenti e del Garante per la protezione dei dati personali.
Il Codice impone alle pubbliche amministrazioni di dialogare fra loro per via informatica o telematica al fine di accelerare le procedure, garantendo comunque legalità e trasparenza, e garantisce, grazie alle nuove tecnologie, una maggiore partecipazione dei cittadini, anche residenti all'estero, alla formazione dei processi decisionali riguardanti la collettività (e-Democracy).
Il Codice riconosce, inoltre, pieno valore probatorio ai documenti informatici conformi ai requisiti prescritti dal d.lgs.. Detti documenti da chiunque trasmessi ad una p.a. con

qualsiasi mezzo telematico o informatico, compreso il fax, 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. Il documento informatico inoltrato per via telematica si intende inviato dal mittente se trasmesso, e si intende consegnato al destinatario, se disponibile all'indirizzo elettronico da questi dichiarato.
Il documento cartaceo è dunque destinato a rappresentare non più la norma bensì l'eccezione. Infatti, la redazione e la copia su supporto cartaceo sarà pertanto consentita solo se necessario e comunque nel rispetto del principio di economicità: spetterà ad un apposito regolamento, da approvarsi entro sei mesi dall'entrata in vigore del Codice, stabilire quali atti amministrativi potranno essere prodotti anche su originale cartaceo.
Il risparmio di spazio e l'abbattimento degli oneri connessi è altresì ottenuto grazie alla facoltà di cui le p.a. dispongono di conservare su supporti informatici qualunque atto, dato o documento, compresi i documenti degli archivi, le scritture contabili, nonché la corrispondenza.

Si segnalano le principali novità del Codice.

- Diritti di cittadini e imprese:

- i cittadini e le imprese hanno diritto di richiedere la *partecipazione al procedimento* amministrativo e di *accedere ai documenti amministrativi* impiegando i nuovi strumenti informatici e di ottenere risposta con i medesimi mezzi;
- tali soggetti hanno inoltre il diritto di *trasmettere atti e documenti* alla p.a. con qualsiasi strumento telematico o informatico, purché sia accertata la fonte di provenienza; sono considerate valide le istanze e le dichiarazioni pervenute per via telematica se sottoscritte mediante firma digitale o nel caso in cui l'interessato sia identificato tramite carta d'identità elettronica o carta nazionale dei servizi;
- a decorrere dal 1° gennaio 2006 le pubbliche amministrazioni centrali consentono l'effettuazione dei *pagamenti* ad esse spettanti, a qualsiasi titolo dovuti, con l'uso delle tecnologie dell'informazione e della comunicazione.

- Obblighi delle p.a.:

- le p.a. sono tenute a utilizzare la posta elettronica per lo scambio on-line di documenti, informazioni e dati relativi alle pratiche di cittadini e imprese, verificandone la provenienza, per evitare il trasferimento cartaceo delle pratiche tra gli uffici e/o le diverse amministrazioni; le comunicazioni sono valide se sottoscritte con firma digitale o firma elettronica qualificata e dotate di protocollo informatizzato;
- le p.a. sono tenute ad adottare, a partire dal 1° gennaio 2007, quale unico standard di accesso ai servizi erogati on-line esclusivamente la Carta d'Identità Elettronica ed alla Carta Nazionale dei Servizi;
- le p.a. hanno l'obbligo sia di trasferire per via telematica i fondi fra amministrazione sia di accettare, a partire dal 1° gennaio 2006, i pagamenti effettuati on-line da cittadini e imprese.

- le p.a. devono, inoltre, riorganizzare i propri siti Internet in modo da individuare una serie di contenuti minimi e necessari, compresa la disponibilità di moduli e formulari per via telematica. In particolare, i siti istituzionali devono contenere i seguenti dati:

  - organigramma con articolazione degli uffici e relative attribuzioni;
  - elenco dei procedimenti svolti, durata di ciascuno e nomi dei relativi responsabili;
  - scadenze e modalità di adempimento dei procedimenti;
  - elenco delle caselle di posta elettronica istituzionali;
  - elenco di tutti i bandi di gara, sottoscritti digitalmente;
  - elenco dei servizi forniti in rete.

  Si allega il testo.

Capo I - Principi generali
Sezione I - Definizioni, finalità e ambito di applicazione
1. Definizioni.
1. Ai fini del presente codice si intende per:
a) allineamento dei dati: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;
b) autenticazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso;
c) carta d'identità elettronica: il documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare;
d) carta nazionale dei servizi: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;
e) certificati elettronici: gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità informatica dei titolari stessi;
f) certificato qualificato: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;
g) certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;
h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;
i) chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;
l) dato a conoscibilità limitata: il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;
m) dato delle pubbliche amministrazioni: il dato formato, o comunque trattato da una pubblica amministrazione;
n) dato pubblico: il dato conoscibile da chiunque;
o) disponibilità: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge;
p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica;
r) firma elettronica qualificata: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica;
s) firma digitale: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;
t) fruibilità di un dato: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;
u) gestione informatica dei documenti: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'àmbito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;
v) originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;
z) pubbliche amministrazioni centrali: le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al *decreto legislativo 30 luglio 1999, n. 300*;
aa) titolare: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;
bb) validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.
2. *Finalità e ambito di applicazione.*
1. Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.
2. Le disposizioni del presente codice si applicano alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del *decreto legislativo 30 marzo 2001, n. 165*, salvo che sia diversamente stabilito, nel rispetto della loro autonomia organizzativa e comunque nel rispetto del riparto di competenza di cui all'articolo 117 della *Costituzione*.
3. Le disposizioni di cui al capo II concernenti i documenti informatici, le firme elettroniche, i pagamenti informatici, i libri e le scritture, le disposizioni di cui al capo III, relative alla formazione, gestione, alla conservazione, nonché le disposizioni di cui al capo IV relative alla trasmissione dei documenti informatici si applicano anche ai privati ai sensi dell'articolo 3 del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*.
4. Le disposizioni di cui al capo V, concernenti l'accesso ai documenti informatici, e la fruibilità delle informazioni digitali si applicano anche ai gestori di servizi pubblici ed agli organismi di diritto pubblico.
5. Le disposizioni del presente codice si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni in materia di protezione dei dati personali approvato con *decreto legislativo 30 giugno 2003, n. 196*.
6. Le disposizioni del presente codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, e consultazioni elettorali.
Sezione II - Diritti dei cittadini e delle imprese
3. Diritto all'uso delle tecnologie.
1. I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni centrali e con i gestori di pubblici servizi statali nei limiti di quanto previsto nel presente codice.
4. Partecipazione al procedimento amministrativo informatico.

1. La partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l'uso delle tecnologie dell'informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*.
2. Ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie dell'informazione e della comunicazione se formato ed inviato nel rispetto della vigente normativa.
5. Effettuazione dei pagamenti con modalità informatiche.
1. A decorrere dal 30 giugno 2007, le pubbliche amministrazioni centrali con sede nel territorio italiano consentono l'effettuazione dei pagamenti ad esse spettanti, a qualsiasi titolo dovuti, con l'uso delle tecnologie dell'informazione e della comunicazione.
6. Utilizzo della posta elettronica certificata.
1. Le pubbliche amministrazioni centrali utilizzano la posta elettronica certificata, di cui al *decreto del Presidente della Repubblica 11 febbraio 2005, n. 68*, per ogni scambio di documenti e informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata.
2. Le disposizioni di cui al comma 1 si applicano anche alle pubbliche amministrazioni regionali e locali salvo che non sia diversamente stabilito.
7. Qualità dei servizi resi e soddisfazione dell'utenza.
1. Le pubbliche amministrazioni centrali provvedono alla riorganizzazione ed aggiornamento dei servizi resi; a tale fine sviluppano l'uso delle tecnologie dell'informazione e della comunicazione, sulla base di una preventiva analisi delle reali esigenze dei cittadini e delle imprese, anche utilizzando strumenti per la valutazione del grado di soddisfazione degli utenti.
2. Entro il 31 maggio di ciascun anno le pubbliche amministrazioni centrali trasmettono al Ministro delegato per la funzione pubblica e al Ministro delegato per l'innovazione e le tecnologie una relazione sulla qualità dei servizi resi e sulla soddisfazione dell'utenza.
8. Alfabetizzazione informatica dei cittadini.
1. Lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni.
9. Partecipazione democratica elettronica.
1. Lo Stato favorisce ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi.
10. Sportelli per le attività produttive.
1. Lo sportello unico di cui all'articolo 3 del *decreto del Presidente della Repubblica 20 ottobre 1998, n. 447*, è realizzato in modalità informatica ed eroga i propri servizi verso l'utenza anche in via telematica.
2. Gli sportelli unici consentono l'invio di istanze, dichiarazioni, documenti e ogni altro atto trasmesso dall'utente in via telematica e sono integrati con i servizi erogati in rete dalle pubbliche amministrazioni.
3. Al fine di promuovere la massima efficacia ed efficienza dello sportello unico, anche attraverso l'adozione di modalità omogenee di relazione con gli utenti nell'intero territorio nazionale, lo Stato, d'intesa con la Conferenza unificata di cui all'articolo 8 del *decreto legislativo 28 agosto 1997, n. 281*, individua uno o più modelli tecnico-organizzativi di riferimento, tenendo presenti le migliori esperienze realizzate che garantiscano l'interoperabilità delle soluzioni individuate.
4. Lo Stato realizza, nell'àmbito di quanto previsto dal sistema pubblico di connettività di cui al *decreto legislativo 28 febbraio 2005, n. 42*, un sistema informatizzato per le imprese relativo ai procedimenti di competenza delle amministrazioni centrali anche ai fini di quanto previsto all'articolo 11.
11. Registro informatico degli adempimenti amministrativi per le imprese.
1. Presso il Ministero delle attività produttive, che si avvale a questo scopo del sistema informativo delle camere di commercio, industria, artigianato e agricoltura, è istituito il Registro informatico degli adempimenti amministrativi per le imprese, di seguito denominato «Registro», il quale contiene l'elenco completo degli adempimenti amministrativi previsti dalle pubbliche amministrazioni per l'avvio e l'esercizio delle attività di impresa, nonché i dati raccolti dalle amministrazioni comunali negli archivi informatici di cui all'articolo 24, comma 2, del *decreto legislativo 31 marzo 1998, n. 112*. Il Registro, che si articola su base regionale con apposite sezioni del sito informatico, fornisce, ove possibile, il supporto necessario a compilare in via elettronica la relativa modulistica.
2. È fatto obbligo alle amministrazioni pubbliche, nonché ai concessionari di lavori e ai concessionari e gestori di servizi pubblici, di trasmettere in via informatica al Ministero delle attività produttive l'elenco degli adempimenti amministrativi necessari per l'avvio e l'esercizio dell'attività di impresa.

3. Con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro delle attività produttive e del Ministro delegato per l'innovazione e le tecnologie, sono stabilite le modalità di coordinamento, di attuazione e di accesso al Registro, nonché di connessione informatica tra le diverse sezioni del sito.
4. Il Registro è pubblicato su uno o più siti telematici, individuati con decreto del Ministro delle attività produttive.
5. Del Registro possono avvalersi le autonomie locali, qualora non provvedano in proprio, per i servizi pubblici da loro gestiti.
6. All'onere derivante dall'attuazione del presente articolo si provvede ai sensi dell'articolo 21, comma 2, della *legge 29 luglio 2003, n. 229*.
Sezione III - Organizzazione delle pubbliche amministrazioni rapporti fra Stato, regioni e autonomie locali
12. Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa.
1. Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione.
2. Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza, secondo le regole tecniche di cui all'articolo 71.
3. Le pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici da esse erogati, qualunque sia il canale di erogazione, nel rispetto della autonomia e della specificità di ciascun erogatore di servizi.
4. Lo Stato promuove la realizzazione e l'utilizzo di reti telematiche come strumento di interazione tra le pubbliche amministrazioni ed i privati.
5. Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.
13. Formazione informatica dei dipendenti pubblici.
1. Le pubbliche amministrazioni nella predisposizione dei piani di cui all'articolo 7-*bis*, del *decreto legislativo 30 marzo 2001, n. 165*, e nell'àmbito delle risorse finanziarie previste dai piani medesimi, attuano anche politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione.
14. Rapporti tra Stato, regioni e autonomie locali.
1. In attuazione del disposto dell'articolo 117, secondo comma, lettera *r*), della Costituzione, lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime.
2. Lo Stato, le regioni e le autonomie locali promuovono le intese e gli accordi e adottano, attraverso la Conferenza unificata, gli indirizzi utili per realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso e per l'individuazione delle regole tecniche di cui all'articolo 71.
3. Lo Stato, ai fini di quanto previsto ai commi 1 e 2, istituisce organismi di cooperazione con le regioni e le autonomie locali, promuove intese ed accordi tematici e territoriali, favorisce la collaborazione interregionale, incentiva la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle soluzioni tecniche ed organizzative, previene il divario tecnologico tra amministrazioni di diversa dimensione e collocazione territoriale.
15. Digitalizzazione e riorganizzazione.
1. La riorganizzazione strutturale e gestionale delle pubbliche amministrazioni volta al perseguimento degli obiettivi di cui all'articolo 12, comma 1, avviene anche attraverso il migliore e più esteso utilizzo delle tecnologie dell'informazione e della comunicazione nell'àmbito di una coordinata strategia che garantisca il coerente sviluppo del processo di digitalizzazione.
2. In attuazione del comma 1, le pubbliche amministrazioni provvedono in particolare a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese, assicurando che l'utilizzo delle tecnologie dell'informazione e della comunicazione avvenga in conformità alle prescrizioni tecnologiche definite nelle regole tecniche di cui all'articolo 71.

3. La digitalizzazione dell'azione amministrativa è attuata dalle pubbliche amministrazioni con modalità idonee a garantire la partecipazione dell'Italia alla costruzione di reti transeuropee per lo scambio elettronico di dati e servizi fra le amministrazioni dei Paesi membri dell'Unione europea.

16. Competenze del Presidente del Consiglio dei Ministri in materia di innovazione e tecnologie.

1. Per il perseguimento dei fini di cui al presente codice, il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie, nell'attività di coordinamento del processo di digitalizzazione e di coordinamento e di valutazione dei programmi, dei progetti e dei piani di azione formulati dalle pubbliche amministrazioni centrali per lo sviluppo dei sistemi informativi:

a) definisce con proprie direttive le linee strategiche, la pianificazione e le aree di intervento dell'innovazione tecnologica nelle pubbliche amministrazioni centrali, e ne verifica l'attuazione;

b) valuta, sulla base di criteri e metodiche di ottimizzazione della spesa, il corretto utilizzo delle risorse finanziarie per l'informatica e la telematica da parte delle singole amministrazioni centrali;

c) sostiene progetti di grande contenuto innovativo, di rilevanza strategica, di preminente interesse nazionale, con particolare attenzione per i progetti di carattere intersettoriale;

d) promuove l'informazione circa le iniziative per la diffusione delle nuove tecnologie;

e) detta norme tecniche ai sensi dell'articolo 71 e criteri in tema di pianificazione, progettazione, realizzazione, gestione, mantenimento dei sistemi informativi automatizzati delle pubbliche amministrazioni centrali e delle loro interconnessioni, nonché della loro qualità e relativi aspetti organizzativi e della loro sicurezza.

2. Il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie riferisce annualmente al Parlamento sullo stato di attuazione del presente codice.

17. Strutture per l'organizzazione, l'innovazione e le tecnologie.

1. Le pubbliche amministrazioni centrali garantiscono l'attuazione delle linee strategiche per la riorganizzazione e digitalizzazione dell'amministrazione definite dal Governo. A tale fine le predette amministrazioni individuano un centro di competenza cui afferiscono i compiti relativi a:

a) coordinamento strategico dello sviluppo dei sistemi informativi, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;

b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi dell'amministrazione;

c) indirizzo, coordinamento e monitoraggio della sicurezza informatica;

d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla *legge 9 gennaio 2004, n. 4*;

e) analisi della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;

f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera *e*);

g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi;

h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale e mandato informatico, e delle norme in materia di sicurezza, accessibilità e fruibilità.

18. Conferenza permanente per l'innovazione tecnologica.

1. È istituita la Conferenza permanente per l'innovazione tecnologica con funzioni di consulenza al Presidente del Consiglio dei Ministri, o al Ministro delegato per l'innovazione e le tecnologie, in materia di sviluppo ed attuazione dell'innovazione tecnologica nelle amministrazioni dello Stato.

2. La Conferenza permanente per l'innovazione tecnologica è presieduta da un rappresentante della Presidenza del Consiglio dei Ministri designato dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie; ne fanno parte il Presidente del Centro nazionale per l'informatica nella pubblica amministrazione (d'ora in poi CNIPA), i componenti del CNIPA, il Capo del Dipartimento per l'innovazione e le tecnologie, nonché i responsabili delle funzioni di cui all'articolo 17.

3. La Conferenza permanente per l'innovazione tecnologica si riunisce con cadenza almeno semestrale per la verifica dello stato di attuazione dei programmi in materia di innovazione tecnologica e del piano triennale di cui all'articolo 9 del *decreto legislativo 12 febbraio 1993, n. 39*.
4. Il Presidente del Consiglio dei Ministri, o il Ministro delegato per l'innovazione e le tecnologie, provvede, con proprio decreto, a disciplinare il funzionamento della Conferenza permanente per l'innovazione tecnologica.
5. La Conferenza permanente per l'innovazione tecnologica può sentire le organizzazioni produttive e di categoria.
6. La Conferenza permanente per l'innovazione tecnologica opera senza rimborsi spese o compensi per i partecipanti a qualsiasi titolo dovuti, compreso il trattamento economico di missione; dal presente articolo non devono derivare nuovi o maggiori oneri per il bilancio dello Stato.
19. Banca dati per la legislazione in materia di pubblico impiego.
1. È istituita presso la Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, una banca dati contenente la normativa generale e speciale in materia di rapporto di lavoro alle dipendenze delle pubbliche amministrazioni.
2. La Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, cura l'aggiornamento periodico della banca dati di cui al comma 1, tenendo conto delle innovazioni normative e della contrattazione collettiva successivamente intervenuta, e assicurando agli utenti la consultazione gratuita.
3. All'onere derivante dall'attuazione del presente articolo si provvede ai sensi dell'articolo 21, comma 3, della *legge 29 luglio 2003, n. 229*.
Capo II - Documento informatico e firme elettroniche; pagamenti, libri e scritture
Sezione I - Documento informatico
20. Documento informatico.
1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici sono validi e rilevanti a tutti gli effetti di legge, se conformi alle disposizioni del presente codice ed alle regole tecniche di cui all'articolo 71.
2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale soddisfa il requisito legale della forma scritta se formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 che garantiscano l'identificabilità dell'autore e l'integrità del documento.
3. Le regole tecniche per la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici sono stabilite ai sensi dell'articolo 71; la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.
4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.
5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.
21. Valore probatorio del documento informatico sottoscritto.
1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.
2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dipositivo di firma si presume riconducibile al titolare, salvo che sia data prova contraria.
3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.
4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:
a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del 13 dicembre 1999 del Parlamento europeo e del Consiglio, ed è accreditato in uno Stato membro;
b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;
c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

22. Documenti informatici delle pubbliche amministrazioni.

1. Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge.

2. Nelle operazioni riguardanti le attività di produzione, immissione, conservazione, riproduzione e trasmissione di dati, documenti ed atti amministrativi con sistemi informatici e telematici, ivi compresa l'emanazione degli atti con i medesimi sistemi, devono essere indicati e resi facilmente individuabili sia i dati relativi alle amministrazioni interessate, sia il soggetto che ha effettuato l'operazione.

3. Le copie su supporto informatico di documenti formati in origine su altro tipo di supporto sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'àmbito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

4. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite ai sensi dell'articolo 71, di concerto con il Ministro per i beni e le attività culturali, nonché d'intesa con la Conferenza unificata di cui all'articolo 8 del *decreto legislativo 28 agosto 1997, n. 281*, e sentito il Garante per la protezione dei dati personali.

23. Copie di atti e documenti informatici.

1. All'articolo 2712 del codice civile dopo le parole: «riproduzioni fotografiche» è inserita la seguente: «, informatiche».

2. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge, se conformi alle vigenti regole tecniche.

3. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata.

4. Le copie su supporto informatico di documenti originali non unici formati in origine su supporto cartaceo o, comunque, non informatico sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è assicurata dal responsabile della conservazione mediante l'utilizzo della propria firma digitale e nel rispetto delle regole tecniche di cui all'articolo 71.

5. Le copie su supporto informatico di documenti, originali unici, formati in origine su supporto cartaceo o, comunque, non informatico sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.

6. La spedizione o il rilascio di copie di atti e documenti di cui al comma 3, esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richieste ad ogni effetto di legge.

7. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71 di concerto con il Ministro dell'economia e delle finanze.

Sezione II - Firme elettroniche e certificatori

24. Firma digitale.

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

25. Firma autenticata.

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale o altro tipo di firma elettronica qualificata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.
2. L'autenticazione della firma digitale o di altro tipo di firma elettronica qualificata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità del certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.
3. L'apposizione della firma digitale o di altro tipo di firma elettronica qualificata da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.
4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.

26. Certificatori.

1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, devono 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.
2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.
3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente codice e le relative norme tecniche di cui all'articolo 71 e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE.

27. Certificatori qualificati.

1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.
2. I certificatori di cui al comma 1, devono inoltre:
a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;
b) utilizzare 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 delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all'articolo 71;
c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;
d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in àmbito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 35, comma 5;
e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi.
3. I certificatori di cui al comma 1, devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al CNIPA, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice.
4. Il CNIPA procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente codice e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.

28. Certificati qualificati.

1. I certificati qualificati devono contenere almeno le seguenti informazioni:
a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;
b) numero di serie o altro codice identificativo del certificato;
c) nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;
d) nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;

e) dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare;
f) indicazione del termine iniziale e finale del periodo di validità del certificato;
g) firma elettronica qualificata del certificatore che ha rilasciato il certificato.
2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale.
3. Il certificato qualificato contiene, ove richiesto dal titolare o dal terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:
a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;
b) limiti d'uso del certificato, ai sensi dell'articolo 30, comma 3;
c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.
4. Il titolare, ovvero il terzo interessato se richiedente ai sensi del comma 3, comunicano tempestivamente al certificatore il modificarsi o venir meno delle circostanze oggetto delle informazioni di cui al presente articolo.
29. Accreditamento.
1. I certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono di essere accreditati presso il CNIPA.
2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27, ed allegare alla domanda oltre ai documenti indicati nel medesimo articolo il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole tecniche.
3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre:
a) avere forma giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, di cui al *decreto legislativo 1° settembre 1993, n. 385*;
b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 del *decreto legislativo 1° settembre 1993, n. 385*.
4. La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.
5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, 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.
6. A seguito dell'accoglimento della domanda, il CNIPA dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal CNIPA stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.
7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.
8. Sono equiparati ai certificatori accreditati ai sensi del presente articolo i certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE.
9. Alle attività previste dal presente articolo si fa fronte nell'àmbito delle risorse del CNIPA, senza nuovi o maggiori oneri per la finanza pubblica.
30. Responsabilità del certificatore.
1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:
a) sull'esattezza e sulla completezza delle informazioni necessarie alla verifica della firma in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;

b) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;
c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi;
d) sull'adempimento degli obblighi a suo carico previsti dall'articolo 32.
2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano affidamento sul certificato stesso, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o non tempestiva sospensione del certificato, secondo quanto previsto. dalle regole tecniche di cui all'articolo 71, salvo che provi d'aver agito senza colpa.
3. Il certificato qualificato può contenere limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel processo di verifica della firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.
31. Vigilanza sull'attività di certificazione.
1. Il CNIPA svolge funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e accreditati.
32. Obblighi del titolare e del certificatore.
1. Il titolare del certificato di firma è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri ed a custodire e utilizzare il dispositivo di firma con la diligenza del buon padre di famiglia.
2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri, ivi incluso il titolare del certificato.
3. Il certificatore che rilascia, ai sensi dell'articolo 19, certificati qualificati deve inoltre:
a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;
b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71, nel rispetto del *decreto legislativo 30 giugno 2003, n. 196*, e successive modificazioni;
c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;
d) attenersi alle regole tecniche di cui all'articolo 71;
e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
f) non rendersi depositario di dati per la creazione della firma del titolare;
g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all'articolo 71;
h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;
i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per dieci anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
k) non copiare, né conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;
l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore;
m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle

informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.
4. Il certificatore è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.
5. Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del *decreto legislativo 30 giugno 2003, n. 196*. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.
33. Uso di pseudonimi.
1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale. Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno dieci anni dopo la scadenza del certificato stesso.
34. Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati.
1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:
a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell'articolo 29; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati;
b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.
2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 72.
3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti di cui all'articolo 71 di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei princìpi generali stabiliti dai rispettivi ordinamenti.
4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche vigenti in materia di firme digitali.
5. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni devono dotarsi di idonee procedure informatiche e strumenti software per la verifica delle firme digitali secondo quanto previsto dalle regole tecniche di cui all'articolo 71.
35. Dispositivi sicuri e procedure per la generazione della firma.
1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:
a) sia riservata;
b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;
c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.
2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71.
3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. L'apposizione di firme con procedura automatica è valida se l'attivazione della procedura medesima è chiaramente riconducibile alla volontà del titolare e lo stesso renda palese la sua adozione in relazione al singolo documento firmato automaticamente.

4. I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza ai sensi dello schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione di cui al comma 5.
5. La conformità dei requisiti di sicurezza dei dispositivi per la creazione di una firma qualificata prescritti dall'allegato III della direttiva 1999/93/CE è accertata, in Italia, in base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. Lo schema nazionale la cui attuazione non deve determinare nuovi o maggiori oneri per il bilancio dello Stato ed individua l'organismo pubblico incaricato di accreditare i centri di valutazione e di certificare le valutazioni di sicurezza. Lo schema nazionale può prevedere altresì la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti afferenti al settore suddetto.
6. La conformità ai requisiti di sicurezza dei dispositivi sicuri per la creazione di una firma qualificata a quanto prescritto dall'allegato III della direttiva 1999/93/CE è inoltre riconosciuta se certificata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 11, paragrafo 1, lettera *b*), della direttiva stessa.
36. Revoca e sospensione dei certificati qualificati.
1. Il certificato qualificato deve essere a cura del certificatore:
a) revocato in caso di cessazione dell'attività del certificatore salvo quanto previsto dal comma 2;
b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;
c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente codice;
d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.
2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo 71.
3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.
4. Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all'articolo 71.
37. Cessazione dell'attività.
1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al CNIPA e informare senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.
2. Il certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. L'indicazione di un certificatore sostitutivo evita la revoca di tutti i certificati non scaduti al momento della cessazione.
3. Il certificatore di cui al comma 1 indica altro depositario del registro dei certificati e della relativa documentazione.
4. Il CNIPA rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 29, comma 6.
Sezione III - Contratti, pagamenti, libri e scritture
38. Pagamenti informatici.
1. Il trasferimento in via telematica di fondi tra pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo le regole tecniche stabilite ai sensi dell'articolo 71 di concerto con i Ministri per la funzione pubblica, della giustizia e dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Banca d'Italia.
39. Libri e scritture.
1. I libri, i repertori e le scritture, ivi compresi quelli previsti dalla legge sull'ordinamento del notariato e degli archivi notarili, di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente codice e secondo le regole tecniche stabilite ai sensi dell'articolo 71.
Capo III - Formazione, gestione e conservazione dei documenti informatici
40. Formazione di documenti informatici.
1. Le pubbliche amministrazioni che dispongono di idonee risorse tecnologiche formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71.

2. Fermo restando quanto previsto dal comma 1, la redazione di documenti originali su supporto cartaceo, nonché la copia di documenti informatici sul medesimo supporto è consentita solo ove risulti necessaria e comunque nel rispetto del principio dell'economicità.
3. Con apposito regolamento, da emanarsi entro 180 giorni dalla data di entrata in vigore del presente codice, ai sensi dell'articolo 17, comma 1, della *legge 23 agosto 1988, n. 400*, sulla proposta dei Ministri delegati per la funzione pubblica, per l'innovazione e le tecnologie e del Ministro per i beni e le attività culturali, sono individuate le categorie di documenti amministrativi che possono essere redatti in originale anche su supporto cartaceo in relazione al particolare valore di testimonianza storica ed archivistica che sono idonei ad assumere.
4. Il Presidente del Consiglio dei Ministri, con propri decreti, fissa la data dalla quale viene riconosciuto il valore legale degli albi, elenchi, pubblici registri ed ogni altra raccolta di dati concernenti stati, qualità personali e fatti già realizzati dalle amministrazioni, su supporto informatico, in luogo dei registri cartacei.
41. Procedimento e fascicolo informatico.
1. Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente.
2. La pubblica amministrazione titolare del procedimento può raccogliere in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della *legge 7 agosto 1990, n. 241*, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata *legge 7 agosto 1990, n. 241*.
3. Ai sensi degli articoli da 14 a 14-*quinquies* della *legge 7 agosto 1990, n. 241*, 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.
42. Dematerializzazione dei documenti delle pubbliche amministrazioni.
1. Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell'articolo 71.
43. Riproduzione e conservazione dei documenti.
1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione sia effettuata in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.
2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali.
3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali.
4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del *decreto legislativo 22 gennaio 2004, n. 42*.
44. Requisiti per la conservazione dei documenti informatici.
1. Il sistema di conservazione dei documenti informatici garantisce:
a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*;
b) l'integrità del documento;
c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;
d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del *decreto legislativo 30 giugno 2003, n. 196*, e dal disciplinare tecnico pubblicato in allegato *B* a tale decreto.
Capo IV - Trasmissione informatica dei documenti
45. Valore giuridico della trasmissione.

1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, 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.
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.
47. Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni.
1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.
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 protocollo informatizzato;
c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71;
d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al *decreto del Presidente della Repubblica 11 febbraio 2005, n. 68*.
3. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni centrali provvedono a:
a) istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ai sensi del *decreto del Presidente della Repubblica 11 febbraio 2005, n. 68*, per ciascun registro di protocollo;
b) utilizzare la posta elettronica per le comunicazioni tra l'amministrazione ed i propri dipendenti, 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.
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*.
2. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata 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.
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.
Capo V - Dati delle pubbliche amministrazioni e servizi in rete
Sezione I - Dati delle pubbliche amministrazioni
50. Disponibilità dei dati delle pubbliche amministrazioni.
1. I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le

norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico.
2. Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della *legge 7 agosto 1990, n. 241*, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo il riconoscimento di eventuali costi eccezionali sostenuti dall'amministrazione cedente; è fatto comunque salvo il disposto dell'articolo 43, comma 4, del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*.
3. Al fine di rendere possibile l'utilizzo in via telematica dei dati di una pubblica amministrazione da parte dei sistemi informatici di altre amministrazioni l'amministrazione titolare dei dati predispone, gestisce ed eroga i servizi informatici allo scopo necessari, secondo le regole tecniche del sistema pubblico di connettività di cui al *decreto legislativo 28 febbraio 2005, n. 42*.
51. Sicurezza dei dati.
1. Le norme di sicurezza definite nelle regole tecniche di cui all'articolo 71 garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati.
2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.
52. Accesso telematico ai dati e documenti delle pubbliche amministrazioni.
1. L'accesso telematico a dati, documenti e procedimenti è disciplinato dalle pubbliche amministrazioni secondo le disposizioni del presente codice e nel rispetto delle disposizioni di legge e di regolamento in materia di protezione dei dati personali, di accesso ai documenti amministrativi, di tutela del segreto e di divieto di divulgazione. I regolamenti che disciplinano l'esercizio del diritto di accesso sono pubblicati su siti pubblici accessibili per via telematica.
53. Caratteristiche dei siti.
1. Le pubbliche amministrazioni centrali realizzano siti istituzionali su reti telematiche che rispettano i princìpi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità dì consultazione, qualità, omogeneità ed interoperabilità.
2. Il CNIPA svolge funzioni consultive e di coordinamento sulla realizzazione e modificazione dei siti delle amministrazioni centrali.
3. Lo Stato promuove intese ed azioni comuni con le regioni e le autonomie locali affinché realizzino siti istituzionali con le caratteristiche di cui al comma 1.
54. Contenuto dei siti delle pubbliche amministrazioni.
1. I siti delle pubbliche amministrazioni centrali contengono necessariamente i seguenti dati pubblici:
a) l'organigramma, l'articolazione degli uffici, le attribuzioni e l'organizzazione di ciascun ufficio anche di livello dirigenziale non generale, nonché il settore dell'ordinamento giuridico riferibile all'attività da essi svolta, corredati dai documenti anche normativi di riferimento;
b) l'elenco delle tipologie di procedimento svolte da ciascun ufficio di livello dirigenziale non generale, il termine per la conclusione di ciascun procedimento ed ogni altro termine procedimentale, il nome del responsabile e l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale, come individuati ai sensi degli articoli 2, 4 e 5 della *legge 7 agosto 1990, n. 241*;
c) le scadenze e le modalità di adempimento dei procedimenti individuati ai sensi degli articoli 2 e 4 della *legge 7 agosto 1990, n. 241*;
d) l'elenco completo delle caselle di posta elettronica istituzionali attive, specificando anche se si tratta di una casella di posta elettronica certificata di cui al *decreto del Presidente della Repubblica 11 febbraio 2005, n. 68*;
e) le pubblicazioni di cui all'articolo 26 della *legge 7 agosto 1990, n. 241*, nonché i messaggi di informazione e di comunicazione previsti dalla *legge 7 giugno 2000, n. 150*;
f) l'elenco di tutti i bandi di gara e di concorso;
g) l'elenco dei servizi forniti in rete già disponibili e dei servizi di futura attivazione, indicando i tempi previsti per l'attivazione medesima.
2. Le amministrazioni che già dispongono di propri siti realizzano quanto previsto dal comma 1 entro ventiquattro mesi dalla data di entrata in vigore del presente codice.

3. I dati pubblici contenuti nei siti delle pubbliche amministrazioni sono fruibili in rete gratuitamente e senza necessità di autenticazione informatica.
4. Le pubbliche amministrazioni garantiscono che le informazioni contenute sui siti siano conformi e corrispondenti alle informazioni contenute nei provvedimenti amministrativi originali dei quali si fornisce comunicazione tramite il sito.
55. Consultazione delle iniziative normative del Governo.
1. La Presidenza del Consiglio dei Ministri può pubblicare su sito telematico le notizie relative ad iniziative normative del Governo, nonché i disegni di legge di particolare rilevanza, assicurando forme di partecipazione del cittadino in conformità con le disposizioni vigenti in materia di tutela delle persone e di altri soggetti rispetto al trattamento di dati personali. La Presidenza del Consiglio dei Ministri può inoltre pubblicare atti legislativi e regolamentari in vigore, nonché i massimari elaborati da organi di giurisdizione.
2. Con decreto del Presidente del Consiglio dei Ministri sono individuate le modalità di partecipazione del cittadino alla consultazione gratuita in via telematica.
56. Dati identificativi delle questioni pendenti dinanzi al giudice amministrativo e contabile.
1. I dati identificativi delle questioni pendenti dinanzi al giudice amministrativo e contabile sono resi accessibili a chi vi abbia interesse mediante pubblicazione sul sistema informativo interno e sul sito istituzionale della rete Internet delle autorità emananti.
2. Le sentenze e le altre decisioni del giudice amministrativo e contabile, rese pubbliche mediante deposito in segreteria, sono contestualmente inserite nel sistema informativo interno e sul sito istituzionale della rete Internet, osservando le cautele previste dalla normativa in materia di tutela dei dati personali.
57. Moduli e formulari.
1. Le pubbliche amministrazioni provvedono a definire e a rendere disponibili anche per via telematica l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà.
2. Trascorsi ventiquattro mesi dalla data di entrata in vigore del presente codice, i moduli o i formulari che non siano stati pubblicati sul sito non possono essere richiesti ed i relativi procedimenti possono essere conclusi anche in assenza dei suddetti moduli o formulari.
Sezione II - Fruibilità dei dati
58. Modalità della fruibilità del dato.
1. Il trasferimento di un dato da un sistema informativo ad un altro non modifica la titolarità del dato.
2. Le pubbliche amministrazioni possono stipulare tra loro convenzioni finalizzate alla fruibilità informatica dei dati di cui siano titolari.
3. Il CNIPA definisce schemi generali di convenzioni finalizzate a favorire la fruibilità informatica dei dati tra le pubbliche amministrazioni centrali e, d'intesa con la Conferenza unificata di cui all'articolo 8 del *decreto legislativo 28 agosto 1997, n. 281*, tra le amministrazioni centrali medesime e le regioni e le autonomie locali.
59. Dati territoriali.
1. Per dato territoriale si intende qualunque informazione geograficamente localizzata.
2. È istituito il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, con il compito di definire le regole tecniche per la realizzazione delle basi dei dati territoriali, la documentazione, la fruibilità e lo scambio dei dati stessi tra le pubbliche amministrazioni centrali e locali in coerenza con le disposizioni del sistema pubblico di connettività di cui al *decreto legislativo 28 febbraio 2005, n. 42*.
3. Per agevolare la pubblicità dei dati di interesse generale, disponibili presso le pubbliche amministrazioni a livello nazionale, regionale e locale, presso il CNIPA è istituito il Repertorio nazionale dei dati territoriali.
4. Ai sensi dell'articolo 17, comma 3, della *legge 23 agosto 1988, n. 400*, con uno o più decreti sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, previa intesa con la Conferenza unificata di cui all'articolo 8 *decreto legislativo 28 agosto 1997, n. 281*, sono definite la composizione e le modalità per il funzionamento del Comitato di cui al comma 2.
5. Ai sensi dell'articolo 17, comma 3, della *legge 23 agosto 1988, n. 400*, con uno o più decreti sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, sentito il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 luglio

1998, n. 281, sono definite le regole tecniche per la definizione del contenuto del repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di successivo aggiornamento dello stesso, per la formazione, la documentazione e lo scambio dei dati territoriali detenuti dalle singole amministrazioni competenti, nonché le regole ed i costi per l'utilizzo dei dati stessi tra le pubbliche amministrazioni centrali e locali e da parte dei privati.
6. La partecipazione al Comitato non comporta oneri né alcun tipo di spese ivi compresi compensi o gettoni di presenza. Gli eventuali rimborsi per spese di viaggio sono a carico delle amministrazioni direttamente interessate che vi provvedono nell'àmbito degli ordinari stanziamenti di bilancio.
7. Agli oneri finanziari di cui al comma 3 si provvede con il fondo di finanziamento per i progetti strategici del settore informatico di cui all'articolo 27, comma 2, della *legge 16 gennaio 2003, n. 3*.
60. Base di dati di interesse nazionale.
1. Si definisce base di dati di interesse nazionale l'insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è utilizzabile dalle pubbliche amministrazioni per l'esercizio delle proprie funzioni e nel rispetto delle competenze e delle normative vigenti.
2. Ferme le competenze di ciascuna pubblica amministrazione, le basi di dati di interesse nazionale costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate. La realizzazione di tali sistemi informativi e le modalità di aggiornamento sono attuate secondo le regole tecniche sul sistema pubblico di connettività di cui all'articolo 16 del *decreto legislativo 28 febbraio 2005, n. 42*.
3. Le basi di dati di interesse nazionale sono individuate con decreto del Presidente del Consiglio dei Ministri, su proposta del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con i Ministri di volta in volta interessati, d'intesa con la Conferenza unificata di cui all'articolo 8 del *decreto legislativo 28 agosto 1997, n. 281*, nelle materie di competenza e sentito il Garante per la protezione dei dati personali. Con il medesimo decreto sono altresì individuate le strutture responsabili della gestione operativa di ciascuna base di dati e le caratteristiche tecniche del sistema informativo di cui al comma 2.
4. Agli oneri finanziari di cui al presente articolo si provvede con il fondo di finanziamento per i progetti strategici del settore informatico di cui all'articolo 27, comma 2, della *legge 16 gennaio 2003, n. 3*.
61. Delocalizzazione dei registri informatici.
1. Fermo restando il termine di cui all'articolo 40, comma 4, i pubblici registri immobiliari possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente codice, secondo le regole tecniche stabilite dall'articolo 71, nel rispetto della normativa speciale e dei princìpi stabiliti dal codice civile. In tal caso i predetti registri possono essere conservati anche in luogo diverso dall'Ufficio territoriale competente.
62. Indice nazionale delle anagrafi.
1. L'Indice nazionale delle anagrafi (INA), di cui all'articolo 1 della *legge 24 dicembre 1954, n. 1228*, è realizzato con strumenti informatici.
Sezione III - Servizi in rete
63. Organizzazione e finalità dei servizi in rete.
1. Le pubbliche amministrazioni centrali individuano le modalità di erogazione dei servizi in rete in base a criteri di valutazione di efficacia, economicità ed utilità e nel rispetto dei princìpi di eguaglianza e non discriminazione, tenendo comunque presenti le dimensioni dell'utenza, la frequenza dell'uso e l'eventuale destinazione all'utilizzazione da parte di categorie in situazioni di disagio.
2. Le pubbliche amministrazioni centrali progettano e realizzano i servizi in rete mirando alla migliore soddisfazione delle esigenze degli utenti, in particolare garantendo la completezza del procedimento, la certificazione dell'esito e l'accertamento del grado di soddisfazione dell'utente.
3. Le pubbliche amministrazioni collaborano per integrare i procedimenti di rispettiva competenza al fine di agevolare gli adempimenti di cittadini ed imprese e rendere più efficienti i procedimenti che interessano più amministrazioni, attraverso idonei sistemi di cooperazione.
64. Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.
1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica.
2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'autenticazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità del soggetto

che richiede l'accesso. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.
3. Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali, con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata di cui all'articolo 8 del *decreto legislativo 28 agosto 1997, n. 281*, è fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi.

65. Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell'articolo 38, commi 1 e 3, del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*, sono valide:
a) se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;
b) ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;
c) ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente e fermo restando il disposto dell'articolo 64, comma 3.
2. Le istanze e le dichiarazioni inviate secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.
3. Dalla data di cui all'articolo 64, comma 3, non è più consentito l'invio di istanze e dichiarazioni con le modalità di cui al comma 1, lettera *c)*.
4. Il comma 2 dell'articolo 38 del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*, è sostituito dal seguente:
«2. Le istanze e le dichiarazioni inviate per via telematica sono valide se effettuate secondo quanto previsto dall'articolo 65 del *decreto legislativo 7 marzo 2005, n. 82*».

Sezione IV - Carte elettroniche

66. Carta d'identità elettronica e carta nazionale dei servizi.

1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica e dell'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento del quindicesimo anno di età, sono definite con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, con il Ministro per l'innovazione e le tecnologie e con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del *decreto legislativo 28 agosto 1997, n. 281*.
2. Le caratteristiche e le modalità per il rilascio, per la diffusione e l'uso della carta nazionale dei servizi sono definite con uno o più regolamenti, ai sensi dell'articolo 17, comma 2, della *legge 23 agosto 1988, n. 400*, adottati su proposta congiunta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del *decreto legislativo 28 agosto 1997, n. 281*, nel rispetto dei seguenti princìpi:
a) all'emissione della carta nazionale dei servizi provvedono, su richiesta del soggetto interessato, le pubbliche amministrazioni che intendono rilasciarla;
b) l'onere economico di produzione e rilascio della carta nazionale dei servizi è a carico delle singole amministrazioni che le emettono;
c) eventuali indicazioni di carattere individuale connesse all'erogazione dei servizi al cittadino, sono possibili nei limiti di cui al *decreto legislativo 30 giugno 2003, n. 196*;
d) le pubbliche amministrazioni che erogano servizi in rete devono consentirne l'accesso ai titolari della carta nazionale dei servizi indipendentemente dall'ente di emissione, che è responsabile del suo rilascio;
e) la carta nazionale dei servizi può essere utilizzata anche per i pagamenti informatici tra soggetti privati e pubbliche amministrazioni, secondo quanto previsto dalla normativa vigente.
3. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento del quindicesimo anno di età, devono contenere:
a) i dati identificativi della persona;

b) il codice fiscale.
4. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento del quindicesimo anno di età, possono contenere, a richiesta dell'interessato ove si tratti di dati sensibili:
a) l'indicazione del gruppo sanguigno;
b) le opzioni di carattere sanitario previste dalla legge;
c) i dati biometrici indicati col decreto di cui al comma 1, con esclusione, in ogni caso, del DNA;
d) tutti gli altri dati utili al fine di razionalizzare e semplificare l'azione amministrativa e i servizi resi al cittadino, anche per mezzo dei portali, nel rispetto della normativa in materia di riservatezza;
e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica.
5. La carta d'identità elettronica e la carta nazionale dei servizi possono essere utilizzate quali strumenti di autenticazione telematica per l'effettuazione di pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalità stabilite con le regole tecniche di cui all'articolo 71, di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.
6. Con decreto del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del *decreto legislativo 28 agosto 1997, n. 281*, sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta di identità elettronica, del documento di identità elettronico e della carta nazionale dei servizi, nonché le modalità di impiego.
7. Nel rispetto della disciplina generale fissata dai decreti di cui al presente articolo e delle vigenti disposizioni in materia di protezione dei dati personali, le pubbliche amministrazioni, nell'àmbito dei rispettivi ordinamenti, possono sperimentare modalità di utilizzazione dei documenti di cui al presente articolo per l'erogazione di ulteriori servizi o utilità.
8. Le tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del *decreto del Presidente della Repubblica 28 luglio 1967, n. 851*, possono essere realizzate anche con modalità elettroniche e contenere le funzionalità della carta nazionale dei servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni.
Capo VI - Sviluppo, acquisizione e riuso di sistemi informatici nelle pubbliche amministrazioni
67. Modalità di sviluppo ed acquisizione.
1. Le pubbliche amministrazioni centrali, per i progetti finalizzati ad appalti di lavori e servizi ad alto contenuto di innovazione tecnologica, possono selezionare uno o più proposte utilizzando il concorso di idee di cui all'articolo 57 del *decreto del Presidente della Repubblica 21 dicembre 1999, n. 554*.
2. Le amministrazioni appaltanti possono porre a base delle gare aventi ad oggetto la progettazione, o l'esecuzione, o entrambe, degli appalti di cui al comma 1, le proposte ideative acquisite ai sensi del comma 1, previo parere tecnico di congruità del CNIPA; alla relativa procedura è ammesso a partecipare, ai sensi dell'articolo 57, comma 6, del *decreto del Presidente della Repubblica 21 dicembre 1999, n. 554*, anche il soggetto selezionato ai sensi del comma 1, qualora sia in possesso dei relativi requisiti soggettivi.
68. Analisi comparativa delle soluzioni.
1. Le pubbliche amministrazioni, nel rispetto della *legge 7 agosto 1990, n. 241*, e del *decreto legislativo 12 febbraio 1993, n. 39*, acquisiscono, secondo le procedure previste dall'ordinamento, programmi informatici a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:
a) sviluppo di programmi informatici per conto e a spese dell'amministrazione sulla scorta dei requisiti indicati dalla stessa amministrazione committente;
b) riuso di programmi informatici sviluppati per conto e a spese della medesima o di altre amministrazioni;
c) acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso;
d) acquisizione di programmi informatici a codice sorgente aperto;
e) acquisizione mediante combinazione delle modalità di cui alle lettere da *a*) a *d*).
2. Le pubbliche amministrazioni nella predisposizione o nell'acquisizione dei programmi informatici, adottano soluzioni informatiche che assicurino l'interoperabilità e la cooperazione applicativa, secondo quanto previsto dal *decreto legislativo 28 febbraio 2005, n. 42*, e che consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto, salvo che ricorrano peculiari ed eccezionali esigenze.

3. Per formato dei dati di tipo aperto si intende un formato dati reso pubblico e documentato esaustivamente.
4. Il CNIPA istruisce ed aggiorna, con periodicità almeno annuale, un repertorio dei formati aperti utilizzabili nelle pubbliche amministrazioni e delle modalità di trasferimento dei formati.
69. Riuso dei programmi informatici.
1. Le pubbliche amministrazioni che siano titolari di programmi applicativi realizzati su specifiche indicazioni del committente pubblico, hanno obbligo di darli in formato sorgente, completi della documentazione disponibile, in uso gratuito ad altre pubbliche amministrazioni che li richiedono e che intendano adattarli alle proprie esigenze, salvo motivate ragioni.
2. Al fine di favorire il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni, ai sensi del comma 1, nei capitolati o nelle specifiche di progetto è previsto ove possibile, che i programmi appositamente sviluppati per conto e a spese dell'amministrazione siano facilmente portabili su altre piattaforme.
3. Le pubbliche amministrazioni inseriscono, nei contratti per l'acquisizione di programmi informatici, di cui al comma 1, clausole che garantiscano il diritto di disporre dei programmi ai fini del riuso da parte della medesima o di altre amministrazioni.
4. Nei contratti di acquisizione di programmi informatici sviluppati per conto e a spese delle amministrazioni, le stesse possono includere clausole, concordate con il fornitore, che tengano conto delle caratteristiche economiche ed organizzative di quest'ultimo, volte a vincolarlo, per un determinato lasso di tempo, a fornire, su richiesta di altre amministrazioni, servizi che consentono il riuso delle applicazioni. Le clausole suddette definiscono le condizioni da osservare per la prestazione dei servizi indicati.
70. Banca dati dei programmi informatici riutilizzabili.
1. Il CNIPA, previo accordo con la Conferenza unificata di cui all'articolo 8 del *decreto legislativo 28 agosto 1997, n. 281*, valuta e rende note applicazioni tecnologiche realizzate dalle pubbliche amministrazioni, idonee al riuso da parte di altre pubbliche amministrazioni.
2. Le pubbliche amministrazioni centrali che intendono acquisire programmi applicativi valutano preventivamente la possibilità di riuso delle applicazioni analoghe rese note dal CNIPA ai sensi del comma 1, motivandone l'eventuale mancata adozione.
Capo VII - Regole tecniche
71. Regole tecniche.
1. Le regole tecniche previste nel presente codice sono dettate, con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e con le amministrazioni di volta in volta indicate nel presente codice, sentita la Conferenza unificata di cui all'articolo 8 del *decreto legislativo 28 agosto 1997, n. 281*, ed il Garante per la protezione dei dati personali nelle materie di competenza, in modo da garantire la coerenza tecnica con le regole tecniche sul sistema pubblico di connettività di cui all'articolo 16 del *decreto legislativo 28 febbraio 2005, n. 42*, e con le regole di cui al disciplinare pubblicato in allegato *B* al *decreto legislativo 30 giugno 2003, n. 196*.
2. Le regole tecniche vigenti nelle materie del presente codice restano in vigore fino all'adozione delle regole tecniche adottate ai sensi del presente articolo.
Capo VIII - Disposizioni transitorie finali e abrogazioni
72. Norme transitorie per la firma digitale.
1. I documenti sottoscritti con firma digitale basata su certificati rilasciati da certificatori iscritti nell'elenco pubblico già tenuto dall'Autorità per l'informatica nella pubblica amministrazione sono equivalenti ai documenti sottoscritti con firma digitale basata su certificati rilasciati da certificatori accreditati.
73. Aggiornamenti.
1. La Presidenza del Consiglio dei Ministri adotta gli opportuni atti di indirizzo e di coordinamento per assicurare che i successivi interventi normativi, incidenti sulle materie oggetto di riordino siano attuati esclusivamente mediante la modifica o l'integrazione delle disposizioni contenute nel presente codice.
74. Oneri finanziari.
1. All'attuazione del presente decreto si provvede nell'àmbito delle risorse previste a legislazione vigente.
75. Abrogazioni.
1. Dalla data di entrata in vigore del presente testo unico sono abrogati:
a) il *decreto legislativo 23 gennaio 2002, n. 10*;

b) gli articoli 1, comma 1, lettere *t*), *u*), *v*), *z*), *aa*), *bb*), *cc*), *dd*), *ee*), *ff*), *gg*), *hh*), *ii*), *ll*), *mm*), *nn*), *oo*); 2, comma 1, ultimo periodo; 6; 8; 9; 10; 11; 12; 13; 14; 17; 20; 22; 23; 24; 25; 26; 27; 27-*bis*; 28; 28-*bis*; 29; 29-*bis*; 29-*ter*; 29-*quater*; 29-*quinquies*; 29-*sexies*; 29-*septies*; 29-*octies*; 36, commi 1, 2, 3, 4, 5 e 6; 51; del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445* (Testo A);
c) l'articolo 26, comma 2, lettere *a*), *e*), *h*), della *legge 27 dicembre 2002, n. 289*;
d) articolo 27, comma 8, lettera *b*), della *legge 16 gennaio 2003, n. 3*;
e) gli articoli 16, 17, 18 e 19 della *legge 29 luglio 2003, n. 229*.
2. Le abrogazioni degli articoli 2, comma 1, ultimo periodo, 6, commi 1 e 2; 10; 36, commi 1, 2, 3, 4, 5 e 6 del *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445* (Testo A), si intendono riferite anche al *decreto legislativo 28 dicembre 2000, n. 443* (Testo B).
3. Le abrogazioni degli articoli 1, comma 1, lettere *t*), *u*), *v*), *z*), *aa*), *bb*), *cc*), *dd*), *ee*), *ff*), *gg*), *hh*), *ii*), *ll*), *mm*), *nn*), *oo*); 6, commi 3 e 4; 8; 9; 11; 12; 13; 14; 17; 20; 22; 23; 24; 25; 26; 27; 27-*bis*; 28; 28-*bis*; 29; 29-*bis*; 29-*ter*; 29-*quater*; 29-*quinquies*; 29-*sexies*; 29-*septies*; 29-*octies*; 51 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).
76. Entrata in vigore del codice.
1. Le disposizioni del presente codice entrano in vigore a decorrere dal 1° gennaio 2006.

Importante parere del Consiglio di Stato sullo schema di decreto legislativo recante il "Codice dell'amministrazione digitale".

NUMERO SCHEDA: 5976

CLASSIFICAZIONE: E-GOVERNMENT

SOTTOCLASSIFICAZIONE: CODICE DELLA AMMINISTRAZIONE DIGITALE

FONTE: CONSIGLIO DI STATO

RIFERIMENTO NORMATIVO: schema di d.lgs. recante il "Codice dell'amministrazione digitale"

NATURA ATTO: PARERE

DATA ATTO: 07/02/2005

NUMERO ATTO: 11995

ORGANO: CONSIGLIO DI STATO

Consiglio di Stato, con parere 7 febbraio 2005, n. 11995, si è pronunciato sullo schema di decreto legislativorecante il "Codice dell'amministrazione digitale", in attuazione della delega contenuta nell'art. 10 della legge 29 luglio 2003, n. 229 "Interventi in materia di qualità della regolazione, riassetto normativo e codificazione- Legge di semplificazione 2001".
Si tratta di un parere molto articolato nel quale il giudizio "favorevole" è subordinato a numerose osservazioni sia di sostanza che di forma.

Si allegano il testo del parere e un commento dell'avv. Andrea Lisi, tratto dal sito scint.it:

Consiglio di Stato, Parere 7 febbraio 2005, n.11995

Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie. Schema di D.Lgs recante il "Codice dell'amministrazione digitale", in attuazione della delega contenuta nell'articolo 10 della legge 29 luglio 2003, n.229, "Interventi in materia di qualità della regolazione, riassetto normativo e codificazione - Legge di semplificazione 2001"

Premesso
1. Lo schema in esame sottopone al parere del CdS il testo di D.Lgs recante il "Codice dell'amministrazione digitale", in attuazione della delega contenuta nell'articolo 10 della legge 229/03 (Interventi in materia di qualità della regolazione, riassetto normativo e codificazione - Legge di semplificazione 2001).
Il termine di scadenza della delega (fissata dopo diciotto mesi dalla data di entrata in vigore della legge 229/03) impone che il provvedimento sia emanato entro il 9 marzo 2005. Il comma 3 della norma di delega consente al Governo di adottare uno o più decreti legislativi recanti disposizioni correttive e integrative, entro dodici mesi decorrenti dalla data di scadenza della delega in questione.
Lo schema, proposto dal Ministro per l'innovazione e le tecnologie, è corredato dei concerti dei Ministri della funzione pubblica e dell'economia e delle finanze, nonché del parere della Conferenza unificata, tutti pervenuti successivamente all'invio del testo dello schema.
Hanno espresso, inoltre, avviso favorevole in ordine allo schema i Ministeri della giustizia, dell'interno, delle comunicazioni e delle attività produttive, nonché il Dipartimento per le politiche comunitarie.
Tale schema costituisce uno dei primi provvedimenti della nuova fase di codificazione finalizzata alla semplificazione e al riordino (ora denominato "riassetto") normativo, sulla quale questo Consiglio ha avuto modo di esprimersi ampiamente in relazione allo schema di D.Lgs concernente il "Codice dei diritti di proprietà industriale", oggetto del parere 2/2004 dell'Adunanza generale. Con parere 11602/04, reso nell'adunanza del 20 dicembre 2004, questa Sezione ha poi espresso il parere sullo schema di D.Lgs recante il "Riassetto delle disposizioni vigenti in materia di consumatori - Codice del consumo".
A tali pareri la Sezione ritiene di poter fare integrale rinvio per tutte le considerazioni generali sul processo di codificazione e per i suggerimenti di metodo rivolti al Governo, contenuti in quella sede.
2. La norma di delega di cui all'articolo 10 della legge 229/03 ha già costituito il fondamento dello schema di D.Lgs recante la 'Istituzione del sistema pubblico di connettività e della rete internazionale della pubblica amministrazione", su cui la Sezione - dopo un primo parere istruttorio del 14 giugno 2004 e i relativi adempimenti - ha espresso parere favorevole con osservazioni nell'adunanza del 30 agosto 2004 (parere 7904/04).
Il D.Lgs non è stato ancora pubblicato alla data della presente adunanza.
Con il parere 7904/04 si è rilevato, tra l'altro, che quel provvedimento - il quale si limita ad istituire il "sistema pubblico di connettività" (SPC e la "rete internazionale della pubblica amministrazione" abrogando un solo comma della legislazione preesistente (il comma 1 dell'articolo 15 della legge 59/1997, sulla Rete unitaria delle pubbliche amministrazioni-RUPA) - non reca il "riassetto in materia di società dell'informazione ", che pure la norma di delega di cui all'articolo 10 della legge 229/03 impone come condizione prioritaria, e non incide sulla ormai ampia normativa esistente in materia di "società dell'informazione" (che costituisce la rubrica della delega di cui all'articolo 10) e di informatica nelle pubbliche amministrazioni.
La Sezione ha, però, rilevato come la stessa delega renda possibile un intervento di riassetto con "uno o più decreti legislativi", ed ha quindi fornito il proprio parere favorevole intendendo -con qualche sforzo interpretativo, di cui la riferente Amministrazione dà atto nella relazione dello schema in oggetto - quello schema di D.Lgs come un intervento parziale, che riordina la materia nella (sola) misura in cui sostituisce l'SPC alla RUPA. La sua natura di "provvedimento di riassetto normativo" (e in ultima analisi il rispetto della norma di delega) era, allora, stata fatta salva a condizione che l'intervento confluisse, poi, nella generale codificazione della materia nel rispetto del comma 1 dell'articolo 10, divenendo "uno" tra i "più" decreti legislativi di riassetto.
Nel merito dello schema, si è segnalata la necessità di integrare quello schema con una o più disposizioni che rendano esplicite ed effettive, sul piano amministrativo, le commendevoli finalità esposte dall'Ufficio legislativo del Ministro per l'innovazione e le tecnologie e contenute, a livello di principio o di dichiarazione di intenti, nello schema, specie in relazione alla necessità di attuare in maniera concreta la lettera b) del comma 1 della nonna di delega (articolo 10 legge 229/03), che - introducendo un criterio incisivo e innovativo - consente di modificare la disciplina vigente "al fine precipuo di garantire la più ampia disponibilità di servizi resi per via telematica" dalle P.A. e "di assicurare ai cittadini e alle imprese l'accesso a tali servizi secondo il criterio della massima

semplificazione degli strumenti e delle procedure necessari e nel rispetto dei principi di uguaglianza, non discriminazione e della normativa sulla riservatezza dei dati personali".
Sempre sulla stessa materia, la Sezione è intervenuta con altri due avvisi che vanno tenuti presenti anche per lo schema in esame: il parere istruttorio 6786/04 reso dall'adunanza del 19 aprile 2004 (che allo stato risulta ancora da ottemperare) sullo schema di regolamento del Ministero dell'interno sull'Indice nazionale delle anagrafi - INA, e il parere n. 7903/04, reso nell'adunanza del 14 giugno 2004, sullo schema di Dpr recante disposizioni per l'utilizzo della posta elettronica certificata, che risulta essere stato approvato in via definitiva dal Consiglio dei Ministri.
3. A differenza dell'intervento parziale di cui sopra, lo schema in oggetto affronta per la prima volta in modo organico il tema dell'utilizzo delle tecnologie dell'informazione e della comunicazione (cd. ICT) nelle pubbliche amministrazioni, nonché della disciplina dei fondamentali principi giuridici applicabili al documento informatico e alla firma digitale.
Si tratta di un'opera di indubbio rilievo sistematico, che può fornire ai cittadini, alle imprese e alle stesse pubbliche amministrazioni uno strumento normativo ampio, tale da orientare in maniera organica i processi di innovazione in atto.
Uno strumento, quello del codice, che - vista la assoluta peculiarità della materia trattata - può contribuire non soltanto alla erogazione di servizi più efficienti e veloci, ma anche a consentire forme innovative di partecipazione alla vita amministrativa e politica. Che può avvicinare i destinatari dell'innovazione (i cittadini, le imprese, la società civile) ai suoi protagonisti (gli amministratori, i funzionari e gli impiegati pubblici), nella nuova "amministrazione digitale", attraverso un intervento più tradizionale e di chiara leggibilità come è un codice, ossia una raccolta organica di disposizioni legislative.
La Sezione ritiene, quindi, di dover dare atto alla riferente Amministrazione di essersi data carico con impegno di tale opera generale di riordino - indicata, sin dal parere n. 7904/04, come l'unica in grado di attuare compiutamente la delega in questione - e di avere effettuato uno sforzo consistente per accelerare il più possibile, fino quasi a forzare, il cambiamento e l'innovazione (e in quest'ottica devono essere lette sia alcune dichiarazioni puramente programmatiche e di principio che la scelta di opzioni particolarmente radicali, che operano l'abbandono irreversibile delle modalità amministrative più tradizionali. Ma, come si dirà, questa impostazione impone un bilanciamento di tali estremi).
Considerato
4. Alla stregua della rilevanza dell'intervento, la Sezione ritiene che l'opera in questione meriti di essere considerata con particolare attenzione e ulteriormente rafforzata, ricercando e segnalando i profili in cui la disciplina può essere resa più completa, ovvero più coerente con il contesto ordinamentale su cui va ad incidere, o più concreta e operativa nel confronti dei cittadini, o più flessibile nell'intervento normativo di riassetto.
La Sezione è, infatti, dell'avviso che lo schema di codice presenti rilevanti peculiarità e aspetti problematici, rispetto al quali le scelte effettuate esigono chiarimenti, o ulteriori sostegni motivazionali, oppure richiedono una riconsiderazione più meditata, da svolgere in collaborazione con le altre amministrazioni competenti (peraltro, i concerti e gli avvisi già resi non appaiono fornire motivazioni specifiche), anche alla stregua delle osservazioni contenute nel presente avviso.
4.1. Prima di esporre puntualmente le osservazioni della Sezione - sia quelle generali sulla struttura dell'intervento che quelle specifiche sui singoli articoli dello schema - si ritiene opportuno raggruppare, qui di seguito, i profili di fondo alla stregua dei quali si invitano il Dipartimento dell'innovazione e le altre amministrazioni interessate - in primo luogo, il Ministero dell'economia e delle finanze, il Dipartimento della funzione pubblica, il Ministero della giustizia e quello dell'interno - ad adeguare lo schema di codice.
In sintesi, le osservazioni della Sezione mirano a conseguire:
- un testo che sia più completo e "leggibile" sull'argomento centrale della disciplina, quello della "amministrazione digitale", che ricomprenda, quantomeno, anche le normative in corso di adozione sul sistema pubblico di connettività - SPC, sull'indice delle anagrafi - INA e sulla posta elettronica certificata (anche recando contestualmente una raccolta organica di norme regolamentari sulla stessa materia) (cfr. infra, il punto 6);
- un testo che affianchi alle enunciazioni programmatiche e di principio, contenute in varie parti del testo, norme precettive -applicabili tramite un processo graduale e guidato di implementazione o, in altri casi, direttamente esecutive - volte all'effettivo perseguimento delle finalità della delega "di garantire la più ampia disponibilità di servizi resi per via telematica dalle pubbliche amministrazioni e dagli altri soggetti pubblici e di assicurare ai cittadini e alle imprese l'accesso a tali servizi secondo il criterio della massima semplificazione degli strumenti e delle procedure necessari e nel rispetto dei

principi di uguaglianza, non discriminazione e della normativa sulla riservatezza dei dati personali" (cfr. infra, il punto 7);
- un testo che non renda incomplete altre discipline già organiche (come quella sulla documentazione amministrativa) e che non tenda ad assorbire la disciplina del procedimento o della documentazione amministrativa, ma che operi il necessario riordino ripensando "a livello informatico" la disciplina sostanziale, nelle sedi sistematicamente proprie (cfr. infra, il punto 8);
- un testo che non rechi una consistente rilegificazione in una materia la quale invece richiede - ontologicamente - la massima flessibilità e che demandi una buona parte della disciplina ad una (possibilmente coeva) raccolta di norme regolamentari (ovvero, eventualmente, a raccolte distinte per i diversi livelli normativi secondari) (cfr. infra, il punto 9);
- un testo che, nell'accelerare il cambiamento, prevenga con misure concrete l'incremento (allo stato ipotizzabile) del fenomeno del digital divide o i rischi che potrebbero derivare dalla troppo rapida scomparsa del documento cartaceo e da una separazione delle discipline della gestione dei documenti da quella degli archivi (cfr. infra, il punto 10) ;
- un testo che, pur nella opportuna centralizzazione di alcuni profili della disciplina, tenga in maggiore considerazione le esigenze di raccordo con le reti regionali e locali integrando - sul modello del sistema pubblico di connettività - a livello statale, la disciplina generale del procedimento amministrativo come disciplina generale valevole anche per le Regioni ma che consenta altresì ai sistemi informatici pubblici regionali e locali di svilupparsi e migliorare le prestazioni, nella compatibilità con l'intero sistema ma nel rispetto dell'autonomia (cfr. infra, il punto 10);
- un testo che, conseguentemente, sia accompagnato dalla previsione di risorse umane e finanziarie adeguate, nonché dalle ulteriori disposizioni di preparazione, attuazione e messa a regime, anche graduale, che consentano una effettiva realizzazione della riforma e delle finalità della delega.
4.2. Considerata la natura strutturale di talune delle osservazioni del presente parere e ritenuto che svariate tra esse debbano essere risolte con la partecipazione delle amministrazioni richiamate, ma constatate altresì la prossimità della scadenza del termine della delega e l'impossibilità di rispettarlo laddove si dovesse procedere ad approfondimenti istruttori, la Sezione suggerisce sin d'ora di valutare l'eventualità di stabilire un congruo termine per l'entrata in vigore dello schema in oggetto (ad esempio, 180 o 240 giorni).
Ciò consentirebbe, oltre che di preparare adeguatamente le amministrazioni e gli operatori ai cambiamenti introdotti, di predisporre la raccolta di norme regolamentari di cui si dirà infra, al punto 9, nonché di far confluire le modificazioni che eventualmente non vi fosse stata la possibilità di apportare con il necessario approfondimento in uno o più decreti legislativi correttivi, consentiti dall'articolo 10, comma 3, della legge 229/03.
In questo modo, entrambi tali tipi di intervento potrebbero entrare in vigore a breve distanza (o addirittura quasi contemporaneamente) al codice in esame.
5. Ai fini di un proficuo completamento dell'iter dello schema, proprio alla stregua del suo notevole rilievo, nell'ulteriore corso del provvedimento (eventualmente anche contemporaneamente all'esame del Parlamento) occorrerà dunque acquisire, in relazione alle osservazioni contenute nel presente parere, gli avvisi delle altre amministrazioni - concertanti e non - sugli aspetti di propria competenza.
5.1. In primo luogo, relativamente al Ministero dell'economia e delle finanze, essendo pervenuti alla Sezione soltanto gli avvisi del Dipartimento della Ragioneria generale dello Stato, dei cui rilievi peraltro lo schema non tiene conto, occorrerà trasmettere il presente parere, oltre che a quel Dipartimento, anche al Dipartimento del tesoro. Il Ministero dell'economia dovrà, infatti, nuovamente pronunciarsi:
- in via generale, sulla concreta 'fattibilità" dei cambiamenti profilati dal nuovo codice (informatizzazione di tutto il sistema della P.A. italiana e dei suoi rapporti coi privati in due anni) senza alcuna contestuale- previsione di risorse aggiuntive e di copertura finanziaria. In particolare, sembra richiedere un esplicito, ulteriore pronunciamento da parte della Ragioneria generale dello Stato l'affermazione della relazione di accompagnamento (pagina 2) secondo cui "questo profondo ammodernamento delle P.A. ... non potrà che attuarsi tramite l'orientamento delle spese ordinarie al perseguimento delle finalità indicate", specificando eventualmente con maggiore precisione -ancorché in termini generali - nel testo e nella relazione finale quali delle finalità attualmente perseguite dovranno essere pretermesse a causa di tale nuovo "orientamento" delle risorse ordinarie;
- specificamente, su svariate disposizioni del testo (e segnatamente gli articoli 5, 6, 7, 9, 11, 13, 15, 16, 31 comma 4, 35, 38, 56, 61 e 62, di cui si dirà caso per caso infra, al punti successivi), le quali, se davvero non recanti spesa, non possono essere intese come disposizioni precettive e dovranno quindi essere interamente riconsiderate in ottemperanza al presente parere, ovvero integrate da altre più concrete disposizioni;

- sulla praticabilità della richiesta "di impegno da parte del Governo per reperire le risorse finanziarie necessarie ad attuare il processo di digitalizzazione in atto", che è stata inserita nel parere della Conferenza unificata del 20 gennaio 2005. Si veda altresì, sempre sulla questione delle risorse finanziarie, il più ampio pronunciamento reso dalla Conferenza unificata il 13 gennaio 2005, allegato al predetto parere del 20 gennaio, secondo il quale, tra l'altro, "qualsiasi intervento di riassetto normativo in materia comunque non è sufficiente se contestualmente non vengono definiti impegni economici e investimenti che dovrebbero trovare copertura nelle leggi finanziarie per dare continuità ai piani di azione per l'e-government italiani ed europei".
Appare, infine, necessario uno specifico pronunciamento degli uffici competenti del Ministero dell'economia riguardo a singole misure previste dal codice in relazione a competenze dirette del Dicastero e, in particolare, un espresso avviso del Dipartimento del tesoro sulla parte riguardante il settore del debito pubblico e le modalità dei pagamenti e dei Dipartimento per le politiche fiscali sui profili relativi alla presentazione della dichiarazione dei redditi per via telematica.
5.2. Inoltre, è necessario che si esprimano sugli specifici punti sollevati con il presente parere il Dipartimento della funzione pubblica, il Ministero dell'interno e il Ministero della giustizia. Ciò al fine di indurre l'Amministrazione proponente a motivare con maggiore ampiezza alcune scelte effettuate con lo schema in questione, nonché ad eventualmente riconsiderarne altri profili.
Per il seguito dell'iter appare innanzitutto necessaria una specifica, ulteriore collaborazione da parte del Dipartimento della funzione pubblica - che pure ha già fornito il suo concerto - in relazione a tutti i profili di incidenza dello schema in oggetto sulla disciplina generale del procedimento amministrativo, nonché alla "perimetrazione" del codice rispetto al testo unico sulla documentazione amministrativa 445/00, di cui si dirà ampiamente infra, ai punti successivi (in particolare ai punti 8 e 9). Molti problemi sollevati dallo schema e molte questioni di connessione tra lo schema di codice in oggetto e il menzionato testo unico non potranno, quindi, essere risolti senza la attiva partecipazione, nella fase successiva dell'iter dello schema, del Dicastero responsabile per la disciplina generale della pubblica amministrazione.
Occorre, inoltre, che per la redazione del testo definitivo si acquisiscano almeno gli avvisi motivati: del Ministero della giustizia su alcune questioni di rilievo, di seguito individuate, e segnatamente su quelle che incidono sulla rilevanza probatoria dei documenti, sull'ordinamento civile con particolare riguardo al rapporti tra privati (articoli 17 e 18), sulla attività notarile; del Ministero dei beni culturali e ambientali per l'archiviazione degli atti; del Ministero dell'interno per quanto attiene alle carte di identità elettronica (il Dpr 445/00 era stato adottato su proposta del Presidente del Consiglio dei Ministri e del Ministro per la funzione pubblica, di concerto con i Ministri dell'interno e della giustizia) e per i rapporti con l'indice nazionale delle anagrafi - INA, che avrebbe dovuto essere costituito con regolamento ministeriale di cui al parere istruttorio di questa Sezione 6786/04 reso dall'adunanza del 19 aprile 2004, che - come si è detto - allo stato risulta ancora da ottemperare.
6. Un primo profilo generale da rimettere alla riconsiderazione del Dipartimento proponente e delle amministrazioni innanzi menzionate è quello della necessità di completare la disciplina organica già contenuta nello schema.
Una delle caratteristiche dell'intervento, infatti, già evidenziata nel precedente parere n. 7904/04 - dovrebbe essere quello della sua esaustività e sistematicità, quantomeno in relazione agli strumenti portanti dell'innovazione digitale nelle pubbliche amministrazioni (cfr., in particolare, la lettera d) della nonna di delega, che impone anche di "realizzare il coordinamento formale del testo delle disposizioni vigenti, apportando, nei limiti di detto coordinamento, le modifiche necessarie per garantire la coerenza logica e sistematica della normativa anche al fine di adeguare o semplificare il linguaggio normativo".
Lo schema in oggetto, invece, si limita a riordinare soltanto una parte della disciplina attualmente vigente, come si evince chiaramente dalla "tabella di corrispondenza" e dalla norma sulle abrogazioni, che in realtà si incentra esclusivamente su due delle molteplici fonti normative riguardanti l'informatizzazione dell'amministrazione pubblica (ossia sul recente DLgs 10/2002 e, soprattutto, sul testo unico sulla documentazione amministrativa, che peraltro costituiva già un riordino della materia: sulle relative problematiche, cfr. infra, i punti 8 e 9). L'effetto di riassetto normativo richiesto dalla delega ne risulta, ad avviso della Sezione, fortemente limitato, non sfruttandosi appieno le potenzialità innovative della delega.
A titolo esemplificativo, una rilevante lacuna - che pure il precedente parere della Sezione 7904/04 aveva raccomandato di evitare - è la mancata considerazione nel codice della disciplina del sistema pubblico di connettività (SPC) di cui al precedente schema di D.Lgs di attuazione dell'articolo 10 della legge 229/03, menzionato retro, al punto 2. Tale sistema costituisce invece, per ammissione dello stesso Dipartimento per l'innovazione, nella relazione a quello schema di D.Lgs, uno degli assi portanti della

riforma, oltre che un esempio di interazione costruttiva tra Stato, Regioni ed autonomie locali e tra i loro sistemi informativi.
In altri termini, se nel precedente parere si affermava che un intervento additivo come la creazione dell'SPC non può prescindere dal "riassetto normativo e codificazione della normativa primaria regolante la materia", che peraltro ispira l'intera legge 229/03, vale anche - e a maggior ragione - il reciproco, perché un codice non può non contenere, al suo interno, una innovazione cosi recente e cruciale come quella di cui al richiamato schema.
Il codice va, altresì, integrato con la disciplina (quantomeno nelle sue linee generali di rango legislativo) dell'Indice nazionale delle anagrafi (INA), per il quale si rinvia alle osservazioni specifiche contenute nel parere istruttorio di questa Sezione 6786/04 e dell'utilizzo della posta elettronica certificata, di cui al parere della Sezione 7903/04.
Dovrebbe poi, in generale, tenersi conto con maggiore organicità delle varie altre normative sulla materia che non risultano comprese nel codice. Per tutte valga, anche qui a titolo di mero esempio, la menzione delle recenti "misure telematiche" contenute nella stessa legge di delega 229/03 in un apposito capo 111 (articoli da 16 a 19) e in particolare la necessità di considerare, nella disciplina codificata, il "Registro informatico degli adempimenti amministrativi per le imprese" (articolo 16 legge 229/03) e la "Consultazione in via telematica", che recepiscono a livello legislativo (senza che, peraltro, risulti essere stata fornita un'ulteriore attuazione a tali previsioni) precise raccomandazioni all'Italia fornite dall'OCSE nel suo Rapporto Regulatory Reform in Italy del 2001; manca, altresì, il recepimento dell'articolo 19 della stessa legge 229, sulla accessibilità informatica dei "Dati identificativi delle questioni pendenti dinanzi al giudice amministrativo e contabile" (che invece risulta in buona parte ormai realizzata). Ma gli esempi potrebbero essere molteplici, sino alla recente legge finanziaria per il 2005 (legge 311/04), ai commi 80, 149, 172, 187, 188, 332 e 333, 374, 380, 381, 382, 383, 384, 385, 429, 431 dell'articolo 1, con le questioni che essi pongono in materia di firma elettronica e di autonomia delle singole amministrazioni.
Infine, appare necessario prendere in considerazione anche la legge di riforma della disciplina generale del procedimento di cui alla legge 241/90 (ormai definitivamente approvata, anche se non ancora pubblicata). La riforma introduce nella legge 241 (come articolo 3bis) un principio generale sull'uso della telematica" (termine che andrebbe coordinato con quelli, diversi, utilizzati dal codice), secondo il quale "Per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati" e reca altri riferimenti (ad esempio, alla conferenza di servizi informatizzata di cui agli articoli 14 e seguenti della stessa legge n. 241 come modificati dalla riforma appena approvata).
Ciò rende ancora più evidente una delle questioni di fondo della materia in esame (di cui si dirà infra, al punto 8): quella dei rapporti tra procedimento amministrativo e disciplina della "digitalizzazione", che il codice risolve - alquanto sommariamente - assorbendo in sé parti della disciplina, senza modificare (o limitandosi ad abrogare) la disciplina "amministrativa" delle stesse procedure.
7. Una seconda questione di tipo strutturale - anch'essa, come la precedente, già rilevata nel precedente parere n. 7904/04 ma non recepita in questa sede - è quella della necessità di accompagnare alle enunciazioni di principio norme direttamente precettive, che non rimettano l'attuazione di tali principi esclusivamente alla volontà (mutevole per definizione) di attuarle da parte delle singole amministrazioni.
Come rilevato dalla migliore dottrina, la presenza di nuovi mezzi di svolgimento dell'attività amministrativa impone, quando le innovazioni lo consentono, il compimento di operazioni di adattamento dei vecchi istituti alle nuove situazioni (si ricordi l'insegnamento di "interrogare i nuovi ordinamenti adoperando gli antichi istituti e modificandoli, quando necessario").
Oltre che di un generale criterio di qualità della produzione normativa, si tratta in questo caso di uno specifico precetto contenuto nella norma di delega più volte richiamato nel parere n. 7904/04.
Come già avvertito nel precedente avviso, se la norma di delega (alla lett. b) del comma 1 dell'articolo 10) consente di innovare la legislazione vigente allo scopo (pressoché esclusivo) di "garantire la più ampia disponibilità di servizi resi . per via telematica" dalle P.A. e di assicurare ai cittadini e alle imprese l'accesso a tali servizi", il decreto delegato non può limitarsi a ribadiretali finalità, ma deve darne concreta ed effettiva attuazione, prevedendo effetti giuridicamente rilevanti per le pubbliche amministrazioni e consentendo, in caso di inerzia o di inadempimento della nuova disciplina, il ricorso da parte di cittadini e imprese agli ordinari strumenti di tutela amministrativa e giurisdizionale. La mancata effettività delle disposizioni generali non potrebbe che ricadere sulla credibilità dell'intera riforma.

In quest'ottica, ad esempio, appare corretto ma non sufficiente inserire, all'inizio del codice, una serie di previsioni programmatiche e di principio (su cui cfr. amplius infra, il punto 12.2), senza prevedere effetti concreti, dal punto di vista della disciplina amministrativa, in materia di "diritti dei cittadini e delle imprese, di documentazione amministrativa, di rilascio degli atti amministrativi, di erogazione dei servizi pubblici on line e di accesso telematico a tali servizi da parte del pubblico.
Né potrebbe sostenersi che le necessarie disposizioni integrative potranno essere introdotte per la prima volta con le "regole tecniche" di cui all'articolo 72 dello schema. Pur se va probabilmente rilevata la natura regolamentare di tali "regole tecniche" (come già riconosciuto dal Dipartimento in sede di adempimento istruttorio sullo schema dell'SPC: cfr. infra, il punto 17, sub articolo 72), le disposizioni integrative in parola si configurano come norme generali, applicabili a tutte le pubbliche amministrazioni, che incidono direttamente sui procedimenti amministrativi e sulle posizioni soggettive dei cittadini e delle imprese. Appare, quindi, necessario che esse siano contenute in una fonte normativa di rango primario, quale è il presente schema di codice. Esso potrà invece, ovviamente, collegarne la concreta vigenza al momento della operatività delle singole "regole tecniche".
Per esempio, un primo modello per rendere effettive alcune delle suindicate finalità (suggerito già dal citato parere n. 7904/04) potrebbe rinvenirsi nella introduzione di un principio generale e precettivo simile a quello contenuto nell'articolo 43 del Dpr 445/00, secondo il quale le amministrazioni pubbliche e i gestori di servizi pubblici non possono richiedere atti o certificati concernenti stati, qualità personali e fatti che risultano elencati all'articolo 46, che siano attestati in documenti già in loro possesso o che comunque esse siano tenute a certificare".
Altra possibilità sarebbe quella di prevedere la liberazione dei cittadini e delle imprese dall'onere di fornire ad una amministrazione pubblica, in generale o per determinate procedure, tutti gli atti o i documenti comunque reperibili da altre amministrazioni in via telematica o informatica (per esempio, limitatamente a determinate categorie di soggetti pubblici, a causa del sistema di interconnessione: un caso tipico potrebbe essere quello dei titoli, da esibire in un concorso pubblico, o in una gara di appalto, che fossero già in possesso di altre amministrazioni, che attualmente continuano ad essere richiesti come necessario elemento integrativo della domanda).
La riconsiderazione di questo profilo molto rilevante dell'impianto dovrebbe indurre a modificare anche la asserzione della relazione di accompagnamento (pag. 2) secondo cui "il D.Lgs non comporta alcuna spesa o onere per il bilancio pubblico" e che "siffatta circostanza deriva dalla stessa natura di codice rivestita dal testo, e dunque dalle stesse finalità generali e programmatiche che essa presenta".
Come si è detto, la natura del codice e la specifica norma di delega impongono, al contrario, una precettività dell'intervento codicistico, che, si ripete, può innovare solo al fine di "garantire -con norme direttamente applicabili e non solo programmatiche - la più ampia disponibilità di servizi resi per via telematica dalle pubbliche amministrazioni e dagli altri soggetti pubblici", o di "assicurare - anche qui con norme non solo "generali e programmatiche" - ai cittadini e alle imprese l'accesso a tali servizi ".
Di ciò dovrà tenere specificamente conto anche il Ministero dell'economia, nell'adempiere al richiesto intervento sul seguito dell'iter dello schema, quantomeno nel prevedere un obbligo espresso di distogliere le risorse per "spese ordinarie" (da individuare specificamente) e di riorientarle a favore dell'innovazione digitale (cfr. retro, il punto 4).
Inoltre, accanto alle disposizioni integrative di cui si è detto andrebbe altresì prevista una specifica normativa attuativa per l'effettiva (e verosimilmente graduale) messa in pratica delle finalità enunciate dal codice (soprattutto dal suo Capo 1), prevedendo, oltre alla individuazione delle risorse nell'ambito delle "spese ordinarie" (se tale procedimento è ritenuto corretto dal Ministero responsabile), la definizione in concreto di programmi di sperimentazione, di formazione e di graduale "messa a regime" delle innovazioni annunciate.
8. Le problematiche sinora esposte dovrebbero condurre a valutare l'opportunità di un consistente rafforzamento ed ampliamento della portata del codice in oggetto.
D'altro canto, non può tacersi di un terzo profilo problematico (ampiamente messo in evidenza dai primi due pareri di questo CdS sulla nuova fase della codificazione, il parere n. 2/2004 dell'Adunanza generale e il n. 11602/2004 della Sezione): quello della "perimetrazione" del codice e, in generale, del rapporto tra la disciplina sulla digitalizzazione dell'amministrazione e quella sul procedimento amministrativo digitalizzato.
In generale, si deve osservare che nel codice non si prevede quale delle fasi del procedimento amministrativo (in genere e non solo statale), dalla fase di iniziativa o comunicazione di avvio del procedimento, alla fase della istruttoria (produzione o comunicazione di atti o di avvenuta recezione di atti), alla fase determinativa (si pensi a procedure automatizzate, che limitano la discrezionalità quasi ad azzerarla, nelle quali la volontà è quasi del computer o del programma), alla fase di integrazione

della efficacia (si pensi alla comunicazione, recettizietà o pubblicità rese con il mezzo informatico), possa avvenire con modalità informatiche e telematiche. Nulla stabilendosi in relazione alle varie fasi del procedimento amministrativo, non si percepisce il vantaggio che dall'informatizzazione del procedimento può derivare al cittadino e utente di pubblici servizi.
8.1. Il problema della perimetrazione del codice si pone, poi, con particolare delicatezza nei confronti di una normativa anch'essa già riordinata di recente, che sta fornendo buoni risultati: quella del testo unico sulla documentazione amministrativa (Dpr 445/00 e connessi testi a - D.Lgs 443/00 - e b - Dpr 444/00).
Appare, anzi, quantomeno singolare che la norma sulle abrogazioni (articolo 75) si incentri come si è detto esclusivamente sul D.Lgs 10/02 e sul Tu 445/00, cosi concentrando (e limitando) la propria opera di "riassetto" su una normativa che in realtà era stata già riordinata di recente, tralasciando invece tutte le altre norme sulla materia, presenti, spesso in modo asistematico, in molteplici fonti dell'ordinamento.
Questo CdS considera, poi, con preoccupazione il rischio che si pervenga nuovamente alla frammentazione di una disciplina che, dopo lunga attesa (di oltre trent'anni) e svariati tentativi, era stata riordinata organicamente. In relazione allo schema di quel testo unico, la Sezione (parere n. 147/00) aveva, tra l'altro, apprezzato la scelta di raccogliere in un'unica fonte normativa sia le disposizioni relative alla tradizionale documentazione amministrativa cartacea (certificati, autocertificazioni, dichiarazioni, etc.) che quelle relative alla documentazione informatica (documento elettronico, firma digitale, etc.), fornendo ai cittadini una sede unitaria della disciplina e favorendo in tal modo anche la progressione da un modello di documentazione ad un altro. In proposito, il citato parere aveva anche affermato che l'informatica costituisce uno strumento al servizio dei cittadini, delle imprese e delle pubbliche amministrazioni e che va direttamente integrata nella disciplina dei relativi procedimenti amministrativi.
Nel codice in oggetto sembra, invece, che si estrapoli la disciplina di quel testo unico che riguarda l'amministrazione digitale. Senza menzionare il fatto che nel testo unico citato si eliminano norme regolamentari per trasformarle in norme tecniche, mentre nello schema in esame si rilegificano norme regolamentari, con conseguenze negative per la flessibilità dell'intera disciplina (sulla possibilità di intervenire anche a livello subprimario, cfr. infra, il punto 9).
La disciplina sembra, dunque, separarsi nuovamente e al tempo stesso irrigidirsi, laddove sarebbe possibile, invece, integrare e rafforzare la precedente raccolta normativa organica, con un'opera di novella cui si potrebbe provvedere nell'ambito dell'esercizio di questa stessa delega:
- attraverso lo stesso codice, eventualmente con un titolo separato ed esclusivamente dedicato alla novella di un'altra disciplina organica;- ovvero, preferibilmente, con un separato e contestuale D.Lgs di novella che modifichi i profili di quella normativa organica da migliorare e ammodernare;- peraltro, coevamente al codice in oggetto, si potrebbe provvedere anche per il livello regolamentare, prevedendo eventualmente un distinto ma contemporaneo intervento anche sulle norme di rango secondario contenute in quel testo unico.
8.2. Quello dei rapporti con il testo unico sulla documentazione amministrativa rappresenta un esempio, ancorché il più rilevante, del rapporto tra due ambiti di materie sopra individuate (la digitalizzazione dell'amministrazione e il procedimento amministrativo digitalizzato) i cui confini andrebbero definiti con maggiore visione sistemica dell'ordinamento, operando - di concerto con il Dipartimento della funzione pubblica - una generale riconsiderazione sulla natura strumentale della "digitalizzazione" rispetto al servizio reso dalle amministrazioni pubbliche o ai provvedimenti da queste adottati (e non viceversa) e, più in generale, sulla strumentalità del cambiamento portato dalle tecnologie dell'informazione rispetto al più generale cambiamento necessario (e certamente in parte già in atto) nella fonction publique del nostro Paese.
Da tale riconsiderazione - da effettuarsi, semmai, anche con gli interventi correttivi di cui al comma 3 dell'articolo 10 di delega, calibrando eventualmente su tali interventi l'entrata in vigore dell'intera riforma (cfr. retro, il punto 5.2) - potrebbe conseguire un duplice effetto positivo. La riferente Amministrazione, senza rinunciare alla capacità innovativa del codice, potrebbe in tal modo:
- da un lato, modificare la sede sistematica di taluni suoi interventi e, con il medesimo D.Lgs in oggetto o con un altro decreto, collocare alcune delle disposizioni ora comprese nel codice in altri contesti normativi organici o generali (come ad esempio la legge generale sul procedimento ovvero il testo unico della documentazione amministrativa);
- dall'altro (ri)trasferire altre disposizioni contenute nello schema in una raccolta di norme di natura regolamentare, da redigere contemporaneamente all'intervento di rango primario, conservando una

maggiore visione d'insieme delle varie politiche perseguite senza asservirle tutte a quella della pur fondamentale "digitalizzazione" dell'amministrazione.
In ogni caso, non si potrebbe in alcun modo prescindere dalla necessità di inserire, all'interno dell'abrogando (parzialmente) testo unico sulla documentazione amministrativa, disposizioni di raccordo con il codice in esame, che rendano più chiara e leggibile all'utente l'esistenza di una seconda, diversa disciplina in luogo di quella unitaria oggi vigente.
9. Un ulteriore profilo di rafforzamento complessivo dell'intervento è quello relativo ai rapporti tra i diversi livelli di fonti normative e in particolare tra legge e regolamento, di cui si è più volte fatta menzione nel punti precedenti.
Se la nuova fase di "codificazione" di cui alla legge 229/03 si caratterizza, rispetto ai "testi unici misti" di cui all'abrogato articolo 7 della legge 50/1999, dall'abbandono dell'inclusione di disposizioni di rango regolamentare e dalla capacità innovativa attribuita oggi al legislatore (primario) delegato, ciò non significa che il codice debba necessariamente operare, nel nome della unitarietà della disciplina, la "rilegifiazione" di molte norme ora previste al più flessibile livello regolamentare, come invece fa il codice in oggetto (basti osservare la tabella di corrispondenza e il cospicuo numero di norme regolamentari che trovano ora sede tra le disposizioni del codice, aventi natura legislativa).
Peraltro, la rilegificazione appare particolarmente controindicata proprio in una materia come quella in oggetto, in cui anzi alcune disposizioni tecniche, a rapidissima evoluzione, dovrebbero essere rese ancora più flessibili (un meccanismo analogo è previsto, correttamente, dal testo unico sulla documentazione amministrativa). Appare, infatti, limitativo volere codificare la fase attuale (fermatasi, allo stato della tecnica, alla firma digitale, di cui la dottrina afferma la artificiosità), mentre in un futuro, forse anche imminente, potrebbero raggiungersi diverse e più efficaci modalità di esternazione degli atti o di apposizione di sigilli, etc. (si pensi alla impronta del dito, alla identificazione attraverso l'iride, alla certezza del dna per la identità dei soggetti, alla videoconferenza certificata).
Questo CdS ha più volte affermato la possibilità e l'opportunità - specialmente in casi come quello di specie - di emanare contemporaneamente al codice, di rango primario, una raccolta organica di norme secondarie, che trova anche uno specifico fondamento autorizzatorio nella stessa legge 229/03 (cfr. il più volte citato parere n. 2/04 dell'Adunanza generale).
Alla stregua di tale disposizione generale, e in considerazione del fatto che il Governo può in ogni momento avvalersi della propria potestà normativa secondaria, che è una potestà autonoma e non "delegata" (ovviamente, per le sole materie consentite ai sensi dell'articolo 117 Costituzione), può ritenersi che la redazione e l'adozione di un corpus organico di norme di natura regolamentare possa avvenire anche contemporaneamente al processo di adozione del codice e non richieda un ulteriore fondamento legislativo nelle specifiche norme di delega "sostanziale" per le singole materie.
Difatti, la codificazione deve garantire il più possibile non solo l'organicità della materia oggetto del riordino ad un dato livello normativo (quello primario), ma anche la sua completezza. E tale completezza non può prescindere, per le materie in cui la competenza sia rimasta in capo allo Stato, dalla normazione secondaria: non solo quella di natura attuativa e integrativa, ma anche quella di eventuale delegificazione.
Sotto questo profilo, l'introduzione di un corpus normativo compiuto soltanto per la normazione di livello primario e non anche per quella di livello secondario può apparire un limite rilevante per la denunciata rilegificazione dei profili più strettamente connessi, ma anche per la stessa immediata operatività della disciplina, per la sua completezza, per la sua leggibilità, per la sua diretta applicabilità da parte degli operatori e degli interpreti.
Certo, occorrerebbe un accorto sistema di rinvii tra i due testi - che resterebbero comunque separati, a differenza che nei testi unici misti - ma la loro redazione contemporanea potrebbe risultare vantaggiosa anche a questo scopo (anzi, sarebbe auspicabile la pubblicazione sulla medesima Gazzetta Ufficiale di entrambi i testi, a fini di leggibilità e di chiarezza, per offrire agli operatori un unico "testo" con la normativa completa).
Per quanto riguarda, invece, le norme regolamentari già "codificate" nel t.u. n. 445 del 2000, appare sufficiente una mera opera di novella di quella raccolta organica, operando sul suo "testo , contenente le sole norme regolamentari (Dpr n. 444 del 2000).
Un diverso ordine di problemi riguarda il rapporto tra i diversi livelli di fonte secondaria in un eventuale testo unico ad hoc: su tale specifico profilo si rinvia a quanto affermato nel più volte citato parere n. 2/04.
10. Un altro gruppo di rilievi riguarda il ruolo conferito dal codice al documento informatico e la mancata previsione di una dettagliata e credibile normativa transitoria per il progressivo abbandono (e, nell'ottica del codice, per la progressiva scomparsa) del documento cartaceo cosi come oggi conosciuto.

Come affermato retro, al punto 3, la Sezione comprende l'esigenza di "forzare il cambiamento" in cui si muove la riferente Amministrazione, che ha condotto alla scelta di opzioni particolarmente radicali e alla previsione dell'abbandono irreversibile di alcune modalità amministrative più tradizionali.
Tale scelta - pur se astrattamente condivisibile - rischia di produrre rilevanti controindicazioni se non accompagnata da interventi di bilanciamento, allo stato non presenti nel codice. Pertanto, le osservazioni che seguono vanno lette non già nel senso di rallentare il cambiamento o di introdurvi deroghe, ma al contrario nel senso di completarlo con idonee misure di preparazione e di attuazione e di accompagnarlo ad altri interventi di sostegno, a garanzia della sua stessa "fattibilità".
Ad avviso della Sezione, vanno evidenziati quantomeno quattro profili:
- quello della possibile introduzione di disuguaglianze sociali in relazione al diverso livello di dimestichezza con le tecnologie dell'informazione (o, in alternativa, della possibilità di una sostanziale inattuazione delle previsioni de quibus);- quello della non sufficiente considerazione della necessità di raccordo con Regioni e autonomie locali;- quello della possibile perdita del ruolo di certezza e di testimonianza storica del documento amministrativo come sinora conosciuto;- quello della sicurezza e della "tenuta" del nuovo assetto, anche per i casi estremi di crisi "sistemiche", in assenza di previsioni che consentano un funzionamento "non elettronico" della vita pubblica.
10.1. Più di un autore, anche in sede internazionale, ha messo in luce i rischi di una completa "digitalizzazione" dell'amministrazione pubblica in assenza di misure volte a bilanciare tale radicale innovazione. Uno dei pericoli principali -- che fa parte del fenomeno noto come digital divide - è quello che un rilevante numero di cittadini (anziani, disabili, soggetti con basse scolarità, emarginati, abitanti in aree remote o rurali, in ritardo con "l'alfabetizzazione informatica" o semplicemente diffidenti) possa risultare discriminato o addirittura socialmente emarginato da un passaggio radicale e non bilanciato ad un'amministrazione esclusivamente digitale.
Pertanto, il cospicuo numero di previsioni generali e programmatiche presenti nel codice dovrebbe essere accompagnato da interventi specifici di sostegno per i cittadini che non siano in grado di avvalersi delle nuove tecnologie dell'informazione. Alla effettiva attuazione di tali interventi dovrebbe essere condizionata l'intera riforma, eventualmente anche agendo su una diversa disciplina dell'entrata in vigore delle singole disposizioni (in proposito, appare ad esempio piuttosto rigida la previsione di cui all'articolo 58 dello schema: cfr. infra, il punto 15. 1) In altri termini, l'abbandono delle modalità tradizionali di azione amministrativa va necessariamente accompagnato da misure concrete - che richiedono una consona copertura finanziaria e amministrativa - che prevedano azioni adeguate per l'implementazione dei nuovi processi, sia dal punto di vista tecnico che da quello umano (anche con riferimento ad appositi processi fonnativi e di "alfabetizzazione informatica avanzata" degli attuali dipendenti pubblici), nonché da norme transitorie e di raccordo che assicurino la continuità di azione pubblica e scongiurino possibili momenti diimpasse nel passaggio da un sistema all'altro.
10.2. Un ulteriore elemento di perplessità sull'assetto previsto dal codice è che esso appare prescindere, nella sostanza, dal ruolo delle Regioni e delle autonomie locali (soprattutto dei comuni), che costituiscono invece il livello principale sul quale agire per una effettiva erogazione on line dei servizi pubblici - quantomeno di quelli prioritari - a cittadini e imprese.
Proprio a proposito del digital divide si ricorda, ad esempio, che - a differenza di quanto prescritto normativamente dal codice - il documento recante le 'linee guida del Governo per lo sviluppo della Società dell'Informazione" del giugno 2002 prevede espressamente tale azione in via prioritaria (come primo dei dieci obiettivi di e-government a livello locale) e si sofferma esplicitamente sulla necessità di realizzare "centri di servizio a livello territoriale" che possano servire i cittadini con minore dimestichezza con le tecnologie dell'informazione, allo scopo di conseguire entro la legislatura l'obiettivo di avere tutti i servizi prioritari on line, relativi ad almeno il 5 0% della popolazione".
La realizzazione di tale obiettivo, non previsto da un atto di natura normativa, appare alla Sezione, a titolo di esempio, necessariamente antecedente alla entrata in vigore di svariate disposizioni dello schema normativo in oggetto.
Alla stregua di quanto esposto, la Sezione, condividendo le osservazioni contenute nel parere della Conferenza unificata del 20 gennaio 2005, ritiene di raccomandare l'istituzione di un'agenzia nazionale 'federata' per l'e-government, come sede stabile di raccordo tra lo Stato, le Regioni e le autonomie locali".
10.3. Lo schema di codice sembra, inoltre, non tenere nella necessaria considerazione il rilievo del "documento amministrativo" come oggi conosciuto; la sua funzione di certezza e di "evidenza probatoria" che esso ancora assolve nella vita dell'amministrazione e dei rapporti giuridici tra cittadini; il suo contenuto stabile e il suo ruolo di testimonianza storica.

Anche in questo caso, si invita a riconsiderare - di concerto con il Dipartimento della funzione pubblica e con il Ministero dell'interno - la cesura che il codice introduce tra la disciplina in oggetto e quella fornita dal t.u. n. 445 del 2000 in relazione alla tenuta e alla conservazione del sistema di gestione dei documenti ed alla gestione dei flussi documentali e degli archivi (articoli 61 ss.).
Nell'invitare anche in questo caso il Dipartimento ad una maggiore visione d'insieme, che affianchi la gestione dei documenti a quella degli archivi, quella dei protocolli a quella dei sistemi di gestione, si ricorda, a mero titolo di esempio, come recenti riflessioni anche in sedi internazionale (ad esempio, quella che ha portato alla produzione dello standard ISO 15489 sul "records management") dimostrano proprio la necessità di una visione globale di tutto il processo documentario.
Anche in questo caso, la reintroduzione di un raccordo e di un'integrazione tra la policy dell'innovazione digitale e le singole policies amministrative appare alla Sezione una condizione di credibilità della riforma nei confronti dei (non pochi) cittadini più restii ad accettarla, e in ultima analisi un elemento per la riuscita della stessa.
10.4 Sotto un quarto e ultimo profilo, si rileva come il codice, stabilendo il principio di primarietà e originalità (non solo di ausiliarietà o accessorietà) del documento informatico, non preveda misure di accompagnamento a proposito delle esigenze di conservazione, immodificabilità, sicurezza (di archiviazione), problemi tecnici, errori del sistema o dell'operatore umano degli atti informatici delle pubbliche amministrazioni.
Sempre a titolo di esempio, si rileva come la sicurezza sulla firma digitale appaia, allo stato, temporanea, con la conseguente necessità di modificare la chiave privata piuttosto frequentemente (come già accennato retro, al punto 9). Risultano, però, allo studio sistemi più sicuri (quali impronte digitali, impronte retiniche, etc.). Ciò dovrebbe indurre a rendere più flessibili le relative previsioni (anche laddove se ne evitasse la criticata "legificazione"): dovrebbe, pertanto, valutarsi l'opportunità di inserire fin d'ora previsioni che limitino la normativa introdotta fino al momento in cui sarà tecnicamente possibile imprimere agli atti e ai documenti informatici impronte antropometriche (o, in ogni caso, sistemi più sicuri di quelli ora previsti), che consentano senza possibilità di errore di stabilire la provenienza, la firma, etc.
11. Una volta esposte le osservazioni di fondo di cui ai punti precedenti, vanno ora formulati specifici rilievi sull'articolato, anche al fine di facilitare la valutazione di alcuni degli aspetti problematici generali dianzi evidenziati e di accelerare l'iter dello schema di D.Lgs con riferimento ad altre questioni di particolare importanza nel delineato riassetto della disciplina in materia di informatizzazione e digitalizzazione dell'amministrazione.
Per facilitare la lettura del parere si indicheranno i Capi, le Sezioni e i singoli articoli del codice interessati dalle osservazioni.
12. CAPO 1
12.1 Sezione I
Articolo 1
Occorre preliminarmente osservare che l'articolo 1, dedicato alle definizioni, e gli articoli contenuti nel capo 2 (dal 17 al 36) sono riproduttivi, in linea di massima, di disposizioni contenute nella normativa precedente (in particolare nel Dpr. 445 del 2000), mentre gli articoli dal 2 al 16 non trovano corrispondenti nel precedenti legislativi e regolamentari.
Le definizioni di cui all'articolo 1, imposte dal contenuto tecnico della normativa, non esauriscono tutte quelle contenute nel codice (si veda ad esempio l'articolo 22, comma 2, ai sensi del quale "l'autenticazione della firma digitale o di altro tipo di firma elettronica qualificata consiste nell'attestazione-"). La relazione peraltro afferma che, rispetto alla precedente normativa, talune definizioni sono state eliminate, mentre altre sono state aggiunte.
Può in linea generale osservarsi che non tutte le definizioni coincidono con le accezioni comuni del linguaggio informatico: sarebbe pertanto importante precisare che le definizioni sono valide solo ai fini del significato del codice, e non anche in assoluto. Si pensi per esempio alla distinzione tra il concetto di informatico e quello di digitale. Informatico è ciò che viene formato non con la scrittura a segni grafici, ma ad impulsi elettronici. Digitale è un metodo di rappresentazione della informazione in forma numerica. La normativa esaminata utilizza invece tali espressioni (informatico e digitale) in un senso diverso: informatica o elettronica è la firma debole, mentre digitale è la firma forte, rafforzata dalla certificazione.
Occorre osservare che la Direttiva comunitaria n. 1999/93/CE, che ha introdotto un quadro comunitario per le firme elettroniche, distingue (articolo 2, dedicato alle definizioni) la "firma elettronica" dalla "firma elettronica avanzata".

Anche in considerazione della normativa comunitaria, particolari problemi presenta la distinzione (la graduazione, come si precisa nelle legge di delega) tra i vani generi di firma, ovvero tra le lettere r), s), e t) dell'articolo 1. In proposito, si ricorda che nella delega si fa riferimento al "documento informatico, alla firma elettronica e alla firma digitale" (articolo 10, comma 2, lett. a) della legge n. 229 del 2003). La firma digitale, come risulta dalla definizione e come può dedursi dagli effetti, anche probatori, previsti dagli articoli 17 e 18, è peraltro una specie della firma elettronica qualificata (definita "elettronica avanzata" dalla direttiva comunitaria). Sembra quindi inopportuna la distinzione apparente in tre diverse specie di firma e, se deve essere apprezzata la riduzione a tre delle ipotesi di firma (sono quattro nell'attuale Dpr n. 445 del 2000), sarebbe opportuno un ulteriore chiarimento, nel senso che i tipi di firma sono solo due, la firma elettronica pura e semplice e quella qualificata, di cui la firma digitale è un tipo.
Pertanto, appare opportuno riposizionare le lettere nel seguente ordine: t), s) e r), in modo da anteporre la definizione della firma elettronica "debole" (lett. t), fare seguire quella generale della firma elettronica qualificata (lett. s) e porre alla fine quella della firma digitale come "particolare tipo di firma elettronica qualificata" (lett. r).
Significativa e meritevole di apprezzamento, perché coincidente con la evoluzione della tecnica, è la definizione di indirizzo elettronico, perché introduttiva di una nuova nozione di indirizzo, oltre a quella genericamente deducibile dall'articolo 1335 Cc, in tema di recezione delle dichiarazioni, come ogni luogo che, in quanto inserito nella sfera di dominio o controllo del destinatario, appaia idoneo a consentirgli la ricezione dell'atto e la cognizione del relativo contenuto.
Si segnala, infine che l'aggiunta delle parole "in rete" alla definizione della carta nazionale dei servizi, già contenuta nell'articolo 1, comma 1, lett. bb) del Dpr n. 445 del 2000, può costituire una limitazione ingiustificata alle possibilità di uso della carta stessa.
Articolo 2
Il contenuto dell'articolo 2 potrebbe sembrare in parte esorbitare dalla delega, che elenca tra i propri oggetti: "b) i procedimenti amministrativi informatici di competenza delle amministrazioni statali anche ad ordinamento autonomo", senza alcun riferimento alle competenze procedimentali di Regioni ed enti locali. Va però rilevato che tra gli oggetti della delega rientrano, senza limitazioni: "a) il documento informatico, la firma elettronica e la firma digitale ... c) la gestione dei documenti informatici d) la sicurezza in informatica dei dati e dei sistemi". Le disposizioni relative a tali ambiti, rientrando in larga misura nella materia dell'ordinamento civile e in quella dei livelli essenziali delle prestazioni, si applicano a tutte le pubbliche amministrazioni ed ai privati. e pertanto necessario ridefinire l'ambito di applicazione del codice riportando con chiarezza gli oggetti della delega, eventualmente integrandoli con riferimento ai principi direttivi, che ne individuano le finalità, e chiarire che gli interventi sul procedimenti regionali riguardano solo l'esercizio del potere di coordinamento informatico dei dati delle amministrazioni regionali, secondo quanto previsto dall'articolo 117, secondo comma, lettera r) della Costituzione.
Di grande importanza è il comma 3 dell'articolo in esame, ai sensi del quale, come già prevedeva l'articolo 3 del Dpr n. 445 del 2000, sebbene con diversa espressione, le disposizioni del capo IV (concernenti i documenti informatici, le firme elettroniche, i pagamenti informatici, i libri e le scritture, nonché le disposizioni di cui al capo III, relative a gestione, conservazione, trasmissione dei documenti informatici) si applicano anche ai privati.
Si pone quindi l'esigenza di stabilire quale parte della normativa si applica, e quale non si applica, a soggetti formalmente privati, ma in sostanza pubblici, ai fini di altre discipline. Si ricorda peraltro che l'articolo 3 del Dpr n. 445 del 2000 - norma regolamentare, che non risulta abrogata -individua espressamente i destinatari della normativa del testo unico sulla documentazione amministrativa nei "cittadini dell'Italia e dell'Unione europea, le persone giuridiche, le società di persone, le associazioni, le pubbliche amministrazioni, gli enti, le associazioni e i comitati aventi sede legale in Italia o in uno dei Paesi dell'Unione europea". La mancata riproduzione di tale disposizione nello schema di codice, o comunque l'assenza di una disposizione di rinvio, possono indurre difficoltà interpretative e di coordinamento.
12. 2 Sezione II
Articoli 3-13
Gli articoli in questione destano qualche perplessità: in parte perché affermano diritti non azionabili (articolo 3); in parte perché si limitano a dichiarazioni di intenti e mancano di precettività (articoli 8, 9 e 10); in parte perché rinviano ad altre disposizioni vigenti che non sono poste in discussione dal codice e che, ove si ritenesse necessario, sarebbe bene riprodurre integralmente nel codice (articolo 6); in parte perché enunciano principi che dovrebbero usualmente ispirare l'azione amministrativa e che non

possono, pertanto, comparire in un codice di settore (articolo 10, comma 6); in parte perché pleonastiche o ripetitive (articoli 10, comma l; 12; 13) in quanto ripetono principi già affermati da articoli precedenti, o pacifici, o addirittura precetti costituzionali; in parte perché, come l'articolo 5, prevedono termini che appaiono inadeguati e che, comunque, stante la loro natura ordinatoria, nulla aggiungono alla disposizione cui accedono. Alcune disposizioni sembrano poi comportare l'esigenza di copertura finanziaria per poter trovare effettiva attuazione (articoli 5, 6, 7, 9, 11, 13, 15 e 16: per le considerazioni già svolte sulla questione in generale, cfr. retro, al punto 4).
È pur vero che molte delle finalità ivi enunciate sono commendevoli e condivisibili; tuttavia, adottando uno stile codicistico in senso classico, le disposizioni in esame possono essere ridotte ad indicazioni molto più contenute, che possano avere effetti giuridicamente rilevanti per le pubbliche amministrazioni, eventualmente consentendo, in caso di inerzia o di inadempimento della nuova disciplina, il ricorso da parte di cittadini e imprese agli ordinari strumenti di tutela amministrativa o giurisdizionale (anche su tali considerazioni si rinvia a quanto già rilevato in precedenza).
13. CAPO Il
13. 1 Sezione I
Articoli 17 e 18
Gli articoli 17 e 18, riguardanti il documento informatico e il valore probatorio del documento informatico sottoscritto, contengono disposizioni di grande interesse e importanza.
Essi riprendono concetti già contenuti nel Dpr n. 445 del 2000 (articoli 8 commi 1, 2, 3; 4; 10 e 29 quater). In particolare l'articolo 17 ripete le espressioni e i concetti di validità e rilevanza contenuti in tutte le normative che si sono occupate dell'argomento (cfr. Dpr n. 513 del 1997).
La delega per il coordinamento e il riassetto delle disposizioni vigenti in materia di società dell'informazione, che si applicano, come già previsto dal Dpr n. 445 del 2000, anche al rapporti tra privati, avrebbe potuto costituire l'occasione per realizzare un pieno coordinamento tra le disposizioni in materia informatica e quelle del codice civile in materia di forma degli atti.
Bisogna però prendere atto che il legislatore, in sede di delega, non è intervenuto sulla possibile rivisitazione delle tradizionali figure formali dell'atto pubblico e della scrittura privata, ma solo sull'utilizzo della firma digitale, equiparandola alla sottoscrizione autografa e quindi utilizzando concetti propri delle altre figure. (In realtà ben avrebbe potuto introdurre la forma della scrittura telematica, munita o meno di una firma sicura -o più o meno sicura, ritenendola idonea al perseguimento degli scopi di legge. Basti pensare che il D.Lgs 50/1993, sui contratti a distanza, prevede "contratti conclusi mediante l'uso di strumenti informatici e telematici", con la ulteriore possibilità di distinguere, anche per lo strumento utilizzato, le scritture (non sottoscritte) da quelle sottoscritte, asseverate dalla sottoscrizione). Si rende perciò necessario adeguare lo strumento informatico alle norme vigenti, cercando quanto più possibile di evitare equivoci e ambiguità.
A prescindere dall'antico dibattito dottrinale sulla distinzione tra atto e documento, non si può sottacere che una cosa è il documento, che è il contenente (che è un mezzo di prova), altra cosa è il contenuto o l'atto documentato (il negozio o atto giuridico voluto), altra cosa ancora è la forma, che è elemento essenziale dell'atto o negozio, se prescritta a pena di nullità (articolo 1325 c.c.) e che può consistere nell'atto pubblico o nella scrittura privata, autenticata o non (v. articolo 1350 c.c.).
La affermazione, contenuta nello schema di codice, che sia il documento informatico (sottoscritto con firma digitale) a soddisfare il requisito della forma scritta sembra invece confondere il contenente con il contenuto.
D'altronde, la differenza tra il documento (definito come cosa che serve come mezzo di prova) e l'atto documentato (che può essere narrativo o di dichiarazione di volontà) si evince dalla possibilità che il documento può venire meno (per esempio, perché distrutto), ma non viene meno la possibilità di fornire la prova dell'atto per il quale sia prevista la forma scritta a pena di nullità, ai sensi dell'articolo 2725 c.c.
Sarebbe pertanto opportuno chiarire, data la differenza del mezzo, quale tipo di prova dell'atto può essere fornita nel caso di distruzione del documento informatico che lo contiene.
Inoltre, è opportuna una ulteriore riflessione per raccordare le previsioni di cui agli articoli 17 e 18 con l'articolo 1350 c.c., chiarendo quale sia la forma informatica equivalente all'atto pubblico e alla scrittura privata per gli atti ivi elencati.
Minori problemi in materia crea il vigente articolo 10 del Dpr n. 445 del 2000, che per il documento informatico in sé, a prescindere dalla sottoscrizione, rinvia all'articolo 2712 c.c. e prevede (comma 2) che il documento informatico sottoscritto con firma elettronica soddisfa il requisito della forma scritta, dandosi cosi carico di attribuire un valore a qualsiasi documento informatico, a prescindere dalla forza della firma.

Peraltro, l'idoneità della forma a conseguire un effetto si desume, secondo la dottrina, dall'articolo 121 c.p.c., sulla strumentalità (idoneità allo scopo) delle forme. Si dovrebbe pertanto cercare di affrontare anche nel nuovo codice il tema del valore dell'atto adottato con scrittura telematica anche ove non sia munito di sottoscrizione, laddove sia conosciuto l'autore per la provenienza dal suo indirizzo elettronico, ovvero ove sia sottoscritto con firma elettronica c.d. debole.
Per meglio chiarire tali osservazioni, basti rilevare, a titolo di esempio, che l'articolo 1350 c.c. prevede che determinati atti, per la loro importanza, debbano farsi per atto pubblico o per scrittura privata (anche non autenticata). L'articolo 2657 c.c. stabilisce che la trascrizione non si può eseguire se non in forza di sentenza, di atto pubblico o di scrittura privata con sottoscrizione autenticata o accertata giudizialmente. Sulla base di tali distinzioni è possibile un trasferimento di immobili a mezzo di scrittura privata senza sottoscrizione autenticata, anche se per la trascrizione è poi necessario un atto riproduttivo della forma giusta.
Gli articoli 17 e 18 non chiariscono se sia idonea forma scritta, a tal fine, ai sensi dell'articolo 1350 c.c., la scrittura con firma soltanto elettronica. Anzi, l'articolo 18 sembra escludere tale possibilità, in quanto il secondo comma prevede il soddisfacimento della forma scritta solo per il documento (non per l'atto) con firma elettronica qualificata o firma digitale. Ne discende che la scrittura con firma elettronica (non qualificata) non sembrerebbe integrare la scrittura privata non autenticata di cui all'articolo 1350 c.c., anche se gli autori della scrittura non disconoscono la loro firma. Non si comprende come debba essere considerato l'atto con firma elettronica debole non disconosciuta a norma dell'articolo 215 c.p.c. La previsione della libera valutabilità in giudizio, di cui al primo comma dell'articolo 18, sembra contrastare con il principio desumibile dal codice di rito.
L'articolo 18, comma 2 - fermo restando il problema della scrittura privata sottoscritta con firma elettronica semplice - dovrebbe essere riscritto per evitare ambiguità. Il rinvio all'efficacia di cui all'articolo 2702 c.c. può infatti generare l'equivoco che il documento sottoscritto con firma digitale sia equiparato alla scrittura privata riconosciuta o autenticata, ciò che è positivamente escluso, almeno per l'autentica, dal successivo articolo 22 che disciplina l'autentica notarile. La formulazione potrebbe essere: "Al documento informatico sottoscritto con firma digitale si applica l'articolo 2702 c.c.".
Infatti, alla scrittura autenticata si applicano regole che non valgono invece per la scrittura riconosciuta (come in materia di trascrizione al sensi del richiamato articolo 2657 C.c.). Si deve poi osservare che il meccanismo introdotto della presunzione della riconducibilità dell'utilizzo del dispositivo della firma al titolare, salvo che sia data prova contraria, indebolisce la suddetta equiparazione e genera il dubbio che la fiducia nell'atto informatico, che in questi anni è andata diffondendosi, possa notevolmente ridursi. Sarebbe almeno opportuno individuare il tipo di prova che consente il dísconoscimento secondo un criterio di responsabilità nella conservazione e nell'utilizzo della chiave privata.
Ciò che importa veramente stabilire, in relazione al grado di certezza delle finire e della loro paternità, è su chi incomba l'onere di iniziare il giudizio (oltre che a quali scopi e entro quali limiti), se sull'apparente titolare o su coloro che vogliono fare valere la paternità altrui della firma.
Da un lato, sembra giusto superare i vecchi concetti di falso, strettamente legati al principio di "paternità" della firma e non a quello di "responsabilità" per la firma; dall'altro, occorre fare assoluta chiarezza sulle ipotesi in cui è consentito dimostrare l'assenza di responsabilità (per esempio, errore, violenza, dolo, abuso del mandato, contrarietà a patti interni, abusivo riempimento da parte di colui che aveva la legittimazione). Basti osservare che la dottrina più accreditata, richiamando i principi di auto responsabilità, affidamento, apparenza, rappresentanza, certezza dei rapporti, ha limitato alle sole ipotesi di violenza e di dolo la possibilità di fare valere i vizi della volontà, escludendo per esempio l'errore, cosi come la violazione di patti interni, salva la ipotesi della conoscenza o riconoscibilità da parte del terzo contraente.
Sugli articoli in questione appare, comunque, particolarmente opportuno un pronunciamento del Ministero della giustizia.
Articolo 20
Desta perplessità il rinvio alle regole tecniche per verificare la validità dei duplicati, delle copie e degli estratti del documento informatico in quanto la validità dovrebbe discendere automaticamente dall'identità del testo accompagnata da una semplice attestazione di conformità, indipendentemente dalla forma o dal supporto su cui è trasferito.
Altra perplessità nasce dalla limitazione prevista dal comma 5, che riserva solo ai pubblici ufficiali e ai notai l'attestazione di conformità all'originale di un documento cartaceo trasferito su supporto informatico. Tale disposizione potrebbe avere effetti paralizzanti nell'azione amministrativa e nel processo civile telematico. D'altra parte, non si comprende perché l'attestazione di conformità non possa essere fatta da chi ha formato l'atto o da chi lo riceve.

13.2 Sezione II

Articolo 22

Il comma 2 desta perplessità e dovrebbe essere sostituito con il riferimento alle disposizioni vigenti in materia di autentica notarile, come avviene attualmente nell'articolo 24 del Dpr n. 445 del 2000. La disposizione tra l'altro sembra in contrasto col principio di cui all'articolo 2703 c.c., in quanto il pubblico ufficiale, quando attesta che la sottoscrizione è stata apposta in sua presenza, non accerta alcunché in relazione alla volontà dell'atto contenuto nel documento sottoscritto.

L'accertamento del fatto che l'atto corrisponde alla volontà delle parti e che non è in contrasto con l'ordinamento giuridico è un accertamento che la legge devolve alla competenza del notaio (articolo 47 legge notarile, terzo comma: "Spetta al notaio soltanto d'indagare la volontà delle parti e dirigere personalmente la compilazione integrale dell'atto, ma solo quando si tratta di atto del quale il notaio cura la redazione, formato a sua cura (atto pubblico), non anche quando si tratta di atto formato dalle parti, la cui sola sottoscrizione sia autenticata.

Il notaio, per la efficacia privilegiata della scrittura autenticata, corrispondente a quella dell'atto notarile stricto iure, è tenuto a controllare che la scrittura non sia contraria all'ordine pubblico (articolo 28 legge notarile: per esempio, che non si costituisca una associazione sovversiva), ma va escluso che sussista l'obbligo del notaio di accertare la corrispondenza del contenuto dell'atto alla effettiva volontà delle parti, obbligo che sussiste solo in caso di atto pubblico.

Articolo 24

Non emergono dalla relazione le ragioni per le quali è stata espunta dal comma 4 dell'articolo 27 del Dpr n. 445 del 2000, ivi riprodotto, la previsione che, oltre al divieto di prosecuzione dell'attività, sia intimata "la rimozione degli effetti".

Articolo 28

Pur avendo mantenuto la stessa rubrica dell'articolo 29 del Dpr n. 445 del 2000, l'articolo in esame non fa più cenno alla distinzione tra controllo dell'attività di certificazione e controllo sui certificatori. Dalla relazione non è dato comprendere la portata della modifica.

Articolo 29

E' bene chiarire al comma 2 che tra "gli altri" tutelati dal certificatore è compreso anche il titolare del certificato.

Alla lettera i) è opportuno chiarire quali sono i "servizi di elencazione", altrove non citati né descritti.

Alla lettera m) è opportuno individuare il termine iniziale dal quale decorre l'obbligo di tenuta della registrazione, coordinando la disposizione con l'articolo 30.

Il comma 4 introduce il problema dell'identificazione del soggetto che richiede il certificato qualificato di firma delegando a terzi tale attività, ponendone la responsabilità a carico del certificatore. Tale disposizione, che identifica un problema reale, evidenzia che nel codice manca una disposizione relativa alle modalità con le quali il titolare della firma può rivolgersi al certificatore, agli obblighi che assume nei suoi confronti, alle comunicazioni che è tenuto a fare. Una simile previsione renderebbe più facilmente leggibili tutte le disposizioni relative alla sottoscrizione del documento e alla sua validità.

Articolo 30

Si veda, sub articolo 29, la necessità di coordinamento delle due disposizioni.

Articolo 31

Nella lettera a) del comma 1 è necessario chiarire in qual modo sono individuate le "categorie di terzi, pubblici o privati" nei confronti dei quali l'amministrazione è abilitata ad esercitare l'attività di rilascio dei certificati, quantomeno individuando un criterio di collegamento univoco.

Per quanto attiene al comma 3, occorre sottolineare che l'articolo 31 disciplina la materia già regolata dall'articolo 29-quinquies del Dpr n. 445 del 2000, il quale al quarto comma prevede una disciplina transitoria, in base alla quale sono stati già emessi in Italia certificati elettronici al cui interno è specificato il ruolo del titolare. Sembra opportuno confermare tale disposizione transitoria in attesa dell'emanazione delle nuove regole tecniche.

Sul comma 4, la Sezione condivide i rilievi della Ragioneria Generale dello Stato sulla necessità di una adeguata copertura finanziaria, richiedendo un nuovo pronunciamento del Ministero dell'economia nel seguito dell'iter dello schema.

Articolo 32

L'articolo tratta, come già il 29 sexies del Dpr n. 445 del 2000, dei dispositivi sicuri per la generazione della firma. La sostituzione, al comma 2, del riferimento ai "dati elettronici" col riferimento al "documento" sembra pertanto frutto di una svista in sede di collazione del testo. Nulla ha infatti a che vedere l'articolo 32 con il documento informatico, ma riguarda solo le garanzie di sicurezza per la generazione della firma.

Nel comma 3 è stata aggiunta la frase "e lo stesso renda palese la sua adozione in relazione al singolo documento firmato automaticamente".
Tale espressione sembra complicare oltremodo il procedimento di firma automatica e non chiarisce in che modo il titolare debba agire in concreto. Occorre pertanto eliminarla.
Il comma 6, che come il comma 5 riprende l'articolo 10 del d.lgs. n. 10 del 2002, è stato modificato nel senso che al posto dell'aggettivo "sicura", riferito alla firma, è stato introdotto l'aggettivo "qualificata". La sostituzione potrebbe creare problemi interpretativi, riferendosi l'aggettivo "sicura" a tutte le forme di firma definite come tali dalla direttiva. Sembrerebbe pertanto opportuno ripristinare il testo originale.
Articolo 35
La norma richiede una adeguata copertura finanziaria, su cui dovrà pronunciarsi il Ministero dell'economia e delle finanze.
14. CAPO 111
Si suggerisce di modificare la rubrica del Capo 111 in "Sistema di gestione informatica dei documenti e dei procedimenti delle pubbliche amministrazioni", per omogeneità con la definizione di cui all'articolo 1, comma 1, lettera cc) dello schema.
Sempre con riguardo a tale Capo sembra di dover formulare alcuni rilievi di carattere generale circa la sistematica utilizzata nella ripartizione in Sezioni e nella distribuzione del contenuto normativo fra i vari articoli.
Appare, infatti, indispensabile un coordinamento contenutistico e lessicale della disciplina di tale Capo con la definizione di "gestione informatica dei documenti" di cui all'articolo 1, comma 1, lettera u).
Se, infatti, la gestione informatica dei documenti comprende "l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione e reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici", allora:
- nella rubrica della Sezione 11, dedicata alla "Gestione informatica dei documenti e protocollo informatico", dovrebbe eliminarsi il riferimento al "protocollo informatico", visto che si tratta di uno degli elementi della gestione informatica dei documenti ed è ricompreso in tale più ampia nozione;
- la Sezione III, dedicata alla "Conservazione informatica dei documenti", dovrebbe essere assorbita dalla Sezione 11, visto che anche la conservazione informatica dei documenti rientra nella nozione di gestione informatica dei documenti;
- parimenti, la distinzione, di cui all'articolo 39, comma 1, tra "sistema di gestione informatica dei documenti" e "sistema di conservazione informatica dei documenti" non ha ragion d'essere, perché la gestione informatica comprende l'attività di conservazione informatica;
- è necessario verificare se vada inclusa nella definizione di gestione informatica dei documenti, di cui all'articolo 1, comma 1, lettera u), anche l'attività di "trasmissione interna alle amministrazioni dei documenti informatici" menzionata dall'articolo 39, comma 1, visto che il sistema di gestione informatica, a mente del comma 2, lettera h), dello stesso articolo, deve anche 44consentire lo scambio di informazioni con i sistemi per la gestione dei flussi documentali di altre amministrazioni", e quindi la trasmissione di documenti fra le stesse. Ove l'Amministrazione riferente ritenesse di aderire a tale indicazione, anche la Sezione IV dovrebbe essere assorbita dalla Sezione Il e la rubrica dell'articolo 39 andrebbe cambiata in '"requisiti del sistema per la gestione informatica dei documenti";
- dovrà, infine, valutarsi se non sia preferibile modificare la rubrica della Sezione 1 in "Gestione informatica dei procedimenti", vista la rubrica generale del Capo 3 e considerato che la rubrica della Sezione 2 si riferisca già alla "Gestione informatica dei documenti e protocollo informatico".
14. 1 Sezione I
Articolo 37
Riguardo al primo comma si rileva che, anche dopo l'entrata in vigore del codice, permarranno procedimenti non gestiti con strumenti informatici, come conferma la previsione dell'articolo 38, comma 2. t, quindi, opportuno limitare la portata della disposizione in esame sostituendo l'inciso finale "ai sensi del presente decreto" con una formula più precisa (ad esempio, con le parole "nei casi e nei modi previsti dal presente decreto").
Articolo 38
Con riferimento al disposto del comma 1, l'Amministrazione riferente dovrà valutare se, in considerazione del contenuto della delega di cui all'articolo 10, comma 1, lettera c) della legge n. 229 del 2003 ("prevedere la possibilità di attribuire al dato e al documento informatico contenuto nei sistemi informatici pubblici i caratteri della primarietà e originalità non possa risultare eccedente rispetto

all'ambito della delega l'imposizione alle amministrazioni pubbliche di un obbligo di formare gli originali dei propri documenti con strumenti informatici, in luogo della mera facoltà di ricorrere a tale soluzione.
Fermo quanto rilevato con riguardo al comma 1, relativamente alla previsione di cui al comma 2, l'Amministrazione riferente vorrà valutare se, tenendo conto dell'attuale fase di sviluppo dell'amministrazione digitale, non sia opportuno differire l'entrata in vigore di tale nonna fino ad una data da fissare con il medesimo decreto di cui al comma 3, continuando a consentire, durante un adeguato periodo di transizione, l'utilizzo contemporaneo del documento informatico e di quello cartaceo.
E' necessario sottolineare che la soluzione di cui al comma 3 sembra una di quelle indicate retro, al punto 5, che comporta oneri per il bilancio delle pubbliche amministrazioni.
Articolo 39
Quanto al comma 1, si rinvia alle osservazione innanzi formulate con riguardo all'intero Capo
Al comma 2, alla lettera e), è utile richiamare anche le disposizioni in materia di accesso ai documenti amministrativi, mentre, alla lettera h), lo scambio di informazioni fra amministrazioni va vincolato al rispetto delle disposizioni in materia di protezione dei dati personali. E' preferibile sostituire il termine latino "iter" con un'espressione della lingua italiana.
La portata della lettera i), non presente nel Dpr n. 445 del 2000 e di nuova introduzione, andrebbe meglio chiarita. In particolare si dovrebbe precisare se con essa si intende dire che il flusso di lavoro dei documenti informatici non deve intralciare il procedimento amministrativo.
14. 2 Sezione II
Articolo 40
Il comma 2 andrebbe soppresso, in quanto riproduce nella sostanza il contenuto dell'articolo 39, comma 2, e dell'articolo 48.
Articolo 41
Con riguardo al comma 3 va rilevato che alle diverse aree organizzative omogenee non corrispondono necessariamente altrettanti complessi di unità amministrative dotati di autonomia organizzativa, in quanto la competenza in ordine all'organizzazione delle aree potrebbe essere attribuita dalla legge anche ad organi posti al di fuori delle stesse e in posizione di gerarchia o direzione rispetto agli uffici che le compongono. In tale prospettiva è preferibile modificare l'inciso iniziale del terzo comma, con le parole "Ciascuna area organizzativa omogenea è strutturata in modo tale da assicurare -". Il riferimento alle "'professionalità tecnico archivistiche" va precisato avendo riguardo alle specifiche figure previste dalla contrattazione collettiva.
Va comunque considerato che la disposizione, che ha valore prettamente organizzativo interno e che potrebbe essere migliorata dall'esperienza applicativa concreta, troverebbe forse migliore collocazione in un testo regolamentare.
Articolo 42
Appare opportuno che l'Amministrazione riferente chiarisca, nella relazione, le ragioni per le quali non sono stati riprodotti i commi 3, 4 e 5 dell'articolo 53 del Dpr n. 445 del 2000.
Al comma 5 si richiama il "registro di emergenza", che però non sarebbe più disciplinato dal codice e neppure dal regolamento, vista l'abrogazione dell'articolo 63 del Dpr n. 445 del 2000.
Articolo 43
Nel riferimento normativo va richiamato anche il comma 2 dell'articolo 55 del Dpr n. 445 del 2000.
E' utile che l'Amministrazione riferente precisi, nella relazione, le ragioni per le quali non sono stati riprodotti i commi 3, 4 e 5 del citato articolo 55.
L'Amministrazione vorrà valutare se escludere dalle abrogazioni gli articoli 56 e 57 del Dpr n. 445 del 2000, che sembrano rivestire una certa importanza anche alla luce del nuovo codice.
Articolo 44
Non è chiaro se l'inciso "su qualsiasi tipo di supporto informatico", collocato alla fine del comma 1, si riferisca al trasferimento delle informazioni o al procedimenti conclusi.
Non è dato comprendere, dalla relazione, perché è stato eliminato il comma 1 dell'articolo 62 del Dpr n. 445 del 2000, che consentiva l'individuazione del responsabile del procedimento di salvataggio. Sembra opportuno reintrodurlo o, quantomeno, di richiamare il principio, visto che nel vigente ordinamento non esistono procedimenti che non facciano capo ad un responsabile.
Articolo 45
Si suggerisce di riformulare la parte iniziale della disposizione, che appare di non agevole lettura, e di tenere conto che la gestione informatica dei documenti comprende anche le attività di registrazione di protocollo, segnatura di protocollo, predisposizione di manuali di gestione, salvataggio e conservazione

degli stessi. Potrebbe, pertanto, optarsi per una formulazione alternativa in tale senso: "Le regole tecniche, i criteri e le specifiche delle informazioni, da osservare nelle operazioni di registrazione di protocollo, di segnatura di protocollo, di predisposizione del manuale di gestione, di salvataggio e conservazione dei documenti, nonché in ogni altro aspetto della gestione informatica dei documenti, sono stabiliti".

14.3 Sezione III

Articolo 47

Al comma 1 è opportuno chiarire la portata e l'esatto significato dell'inciso finale "ed in funzione dei principi stabiliti dal presente decreto e delle finalità di cui all'articolo 2, comma 1

Valuti comunque l'Amministrazione se non sia il caso di espungerlo dal testo.

La previsione del comma 2, operando solo per il passato, determina un obbligo di sostituzione immediata dei sistemi di conservazione su supporti fotografici o ottici, già autorizzati dall'articolo 6 del Dpr n. 445 del 2000, che potrebbe trovare non preparate le pubbliche amministrazioni ed i privati che ne facciano uso. Sarebbe, quindi, opportuno continuare a consentire l'utilizzo di tali supporti ancora per una fase transitoria di ragionevole durata.

Articolo 48

Sembra necessario precisare che il sistema di conservazione dei documenti informatici, quando i documenti contengano dati personali, deve garantire anche il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del D.Lgs 30 giugno 2003, n. 196 e dal disciplinare tecnico pubblicato in Allegato B a tale decreto.

Fra i requisiti del sistema andrebbe, inoltre, inclusa la agevole reperibilità del documento.

14.4 Sezione IV

Articolo 49

Poiché la disposizione di cui al comma 2 intende individuare il momento in cui la trasmissione e la consegna del documento informatico sono giuridicamente perfezionate, è preferibile riformularla in modo tale da renderne esplicita la portata e da precisarne il significato, ad esempio sostituendo le parole "se trasmesso" e "se disponibile" con le parole "nel momento in cui ne è completata la trasmissione al proprio gestore" e, rispettivamente, "nel momento in cui diviene effettivamente disponibile, nell'indirizzo da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore". Tale intervento va, comunque, coordinato con quello previsto dall'articolo 3 del decreto del Presidente della Repubblica, recante disposizioni per l'utilizzo della posta elettronica certificata, che sostituisce l'abrogando articolo 14, comma 1, del Dpr n. 445 del 2000.

Articolo 50

Al comma 1 occorre chiarire il significato della formula secondo cui le comunicazioni avvengono "di norma" mediante l'utilizzo della posta elettronica, precisando il parametro che consente all'amministrazione di derogare a tale precetto (es. ragioni tecniche, organizzative o di sicurezza). Appare necessario, inoltre, chiarire che si fa riferimento alle comunicazioni "di documenti", come reso palese dalla rubrica dell'articolo.

Con riguardo alla previsione di cui al comma 3, che impone alle pubbliche amministrazioni l'adozione di determinate soluzioni tecnologiche entro un termine di ventiquattro mesi, è necessario precisare se essa comporti oneri e, in tal caso, la relativa copertura finanziaria.

Articolo 51

Il comma 1 fa riferimento alla nozione di posta elettronica certificata, che dovrebbe essere definita nella disposizione di cui all'articolo 2 del codice.

La nuova formulazione del comma 2, che riproduce e adatta la previsione di cui all'articolo 14, comma 3, del Dpr n. 445 del 2000, potrebbe costituire l'occasione per precisare il significato del rinvio ai "casi consentiti dalla legge", chiarendosi se si alluda ai casi in cui la legge consente la notificazione per mezzo della posta o ai casi in cui la legge ammette l'equipollenza fra notificazione a mezzo posta e invio di posta elettronica certificata.

15. Capo IV

15.1 Sezione I

Articolo 53

Quanto alla formulazione della disposizione di cui al comma 1, va rilevato che anche i limiti posti dalle norme in materia di trattamento dei dati personali sono posti da leggi e regolamenti vigenti. Sembra, quindi, preferibile aggiungere, dopo la parola "regolamenti", l'inciso "ed in particolare dalla disciplina in materia di protezione dei dati personali".

Al comma 2 il richiamo alla "tutela della riservatezza" è più limitato del riferimento alle norme in materia di protezione dei dati personali contenuto nel comma I. E' preferibile un richiamo anche qui

alla "disciplina in materia di protezione dei dati personali". Si suggerisce, inoltre, di valutare se debba richiamarsi anche il limite di cui all'articolo 2, comma 6.
Al comma 3 la parola "costruisce", avendo ad oggetto i "servizi informatici", va sostituita con la parola "predispone", che è lessicalmente più appropriata.
Articolo 54
Quanto al comma 1, occorre coordinarne la disciplina - che riguarda la sicurezza di tutti i dati, anche anonimi, detenuti da pubbliche amministrazioni - con quella di cui all'articolo 39, comma 2, lettera a), che concerne i dati contenuti in documenti informatici, nonché con quella relativa alle misure di sicurezza previste, per il solo trattamento di dati personali, dagli articoli da 31 a 36 del D.Lgs 30 giugno 2003, n. 196 e dal disciplinare tecnico pubblicato in Allegato B a tale decreto.
Non è chiaro, inoltre, il significato del richiamo che il comma 1 opera alle "norme di sicurezza di cui all'articolo 10, comma 6", visto che il citato comma 6 non sembra concernere specificamente la materia delle misure di sicurezza.
La previsione di cui al comma 2 sembra sovrapporsi a quella di cui all'articolo 39, comma 2. L'Amministrazione vorrà, quindi, valutare se l'articolo 54, comma 2, può essere soppresso.
Articolo 55
Nella rubrica dell'articolo la formula "accesso telematico ai dati e documenti pubblici" risulta ambigua, non essendo chiaro se si riferisca ai dati e documenti "pubblici" perché suscettibili di libera diffusione oppure ai dati e documenti "pubblici" perché detenuti da pubbliche amministrazioni.
Si suggerisce, quindi, di fare riferimento ai dati "delle pubbliche amministrazioni".
Quanto al comma 1, è preferibile che almeno la disciplina dell'accesso telematico ai "documenti" amministrativi venga definita non mediante autonomi regolamenti, bensì mediante regolamenti che novellino la vigente disciplina regolamentare della materia, adottata in attuazione della legge n. 241 del 1990.
Potrebbe, infine, essere meglio specificato il significato del riferimento ad un accesso telematico alle "procedure".
Articolo 56
Con riguardo alla disciplina dei siti istituzionali della amministrazioni centrali, delle Regioni e degli enti locali appare opportuno, anche ai sensi dell'articolo 117, comma 2, lettera r), della Costituzione, affidare ad un organismo con mere funzioni consultive e di coordinamento l'esame preventivo dei progetti diretti alla realizzazione e modificazione di tali siti, affinché renda un parere non vincolante circa la conformità degli stessi ai principi e alle caratteristiche di cui al commi 1 e 2.
Nella stessa prospettiva di coordinamento informatico l'Amministrazione riferente vorrà valutare, l'utilità di prevedere l'istituzione e la gestione di un sito unitario che rechi l'elenco generale aggiornato periodicamente dei siti di tutte le amministrazioni pubbliche italiane e i necessari collegamenti (links) al medesimi, come ad esempio già accade in Francia. Con riguardo al comma 1 va chiarito che l'"usabilità", la "reperibilità" e 1 `accessibilità" del sito devono essere di livello elevato (elevata usabilità, etc.).
Articolo 57
Con riguardo al comma 1, lettera a), non sono indicate le ragioni che hanno indotto ad escludere da tale forma di pubblicità gli uffici di livello dirigenziale generale.
Sempre con riferimento al comma 1, le fattispecie di cui alle lettere b) e c) potrebbero essere unificate. In tale prospettiva si suggerisce di aggiungere alla lettera b), dopo le parole 'livello dirigenziale non generale", le parole "il termine per la conclusione di ciascun procedimento ed ogni altro termine procedimentale, il nome del responsabile e l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale, come individuati ai sensi degli articoli 2, 4 e 5 della legge 7 agosto 1990, n. 241".
Alla lettera e) del comma 1 è preferibile sostituire la formula "ogni altra pubblicazione prevista dalla legge 7 giugno 2000, n. 150" con l'inciso 'V messaggi di informazione e di comunicazione previsti dalla legge 7 giugno 2000, n. 150", che individua in termini più precisi le attività disciplinate da tale legge.
Alla lettera j) del comma 1 è opportuno prevedere la pubblicazione, oltre che dei bandi di gara, anche dei bandi di concorso. Sempre con riguardo a tale disposizione è, inoltre, indispensabile precisare i termini per procedere a tale pubblicazione sul sito ed i relativi effetti giuridici.
Ove la pubblicazione sul sito venga intesa come mera forma pubblicitaria integrativa con funzione notiziale, la disposizione in esame dovrebbe chiarire che la pubblicazione del bando sul sito istituzionale non sostituisce le altre forme di pubblicità previste dalla legge, fra cui la pubblicazione nella Gazzetta Ufficiale della Repubblica Italiana, e non determina la decorrenza di termini sostanziali o processuali.

In termini più generali vanno, inoltre, individuate le conseguenze giuridiche di una eventuale omissione di tempestiva pubblicazione sul sito delle informazioni di cui al comma 1 o di errori in tale pubblicazione, chiarendosi, ad esempio, se l'omissione di tale forma pubblicitaria, che è configurata comunque come obbligatoria per l'amministrazione procedente, o eventuali difformità rispetto al contenuto originale del provvedimento, in violazione della previsione di cui al comma 4, o altre inesattezze, rilevino ai fini della eventuale rimessione in termini per errore scusabile o ad altro fine.
Con riguardo alla previsione di cui al comma 2, che impone alle pubbliche amministrazioni di adeguare i loro siti istituzionali entro il termine di ventiquattro mesi, è necessario precisare in che misura essa comporti oneri e, contemporaneamente, la relativa copertura finanziaria; la fissazione di un termine, infatti, rende certa la spesa, diversamente da quanto ritenuto nella relazione tecnicofinanziaria.
Il riferimento al dati "pubblici" contenuto nel comma 3 - come già evidenziato con riguardo all'articolo 55 - non appare idoneo ad individuare le specifiche tipologie di dati cui si fa riferimento.
Articolo 58
Il Consiglio è consapevole della importanza di eliminare tutte le difficoltà connesse con l'acquisizione delle informazioni relative ai procedimenti amministrativi, che spesso impongono sui cittadini oneri defatiganti.
In un sistema in cui fosse stata già completata l'informatizzazione e nel quale esistesse la garanzia dell'accesso diretto al sistema per tutti gli utenti, le disposizioni di cui all'articolo 58 sarebbero pienamente condivisibili.
Peraltro, una disposizione come quella contenuta al comma 2, non accompagnata da altre misure idonee a garantire in concreto la effettiva realizzazione di quanto previsto al comma 1, può produrre rilevanti conseguenze pregiudizievoli, anche in procedimenti di notevole rilevanza sociale nei quali la produzione documentale assume particolare rilievo e non può comunque essere omessa (es. in materia di tutela ambientale) per il solo fatto che sia in qualche misura meno agevole procurarsi il relativo modulo o formulario.
Tenuto conto del grave danno che tale disciplina potrebbe arrecare al buon andamento dell'azione amministrativa e della sproporzione fra l'entità dell'inadempimento formale dell'amministrazione - che potrebbe anche risultare non ad essa imputabile -- e le conseguenze che ne derivano, si ritiene necessario ancorare l'entrata in vigore del comma 2 ad un provvedimento di ricognizione della effettiva avvenuta attuazione delle disposizioni di cui al comma I.
15.2 Sezione II
Articolo 59
Con riguardo al comma 1 si premette che, venendo in considerazione una disposizione definitoria, essa dovrebbe trovare collocazione nell'ambito delle definizioni di cui all'articolo I. In tale sede dovrebbe parimenti precisarsi la nozione di "sistema informativo automatizzato".
Si suggerisce, comunque, di intervenire sulla formulazione della disposizione, non essendo chiaro a quale amministrazione si faccia riferimento con l'aggettivo "propri " riferito ai sistemi informativi automatizzati. In particolare, non è chiaro se la fruibilità consista nella mera possibilità di trasferire il dato all'interno di una stessa amministrazione (fra più sistemi informativi automatizzati gestiti dalla medesima e, quindi, "propri" alla stessa) o, invece, nella possibilità che un dato, trattato nell'ambito del sistema informativo automatizzato di una pubblica amministrazione, possa essere trasferito al sistema informativo automatizzato di altre pubbliche amministrazioni.
Quanto alla previsione di cui al comma 2, ne sono oscuri il fondamento e la portata, che è opportuno chiarire. In proposito si evidenzia che tale disposizione, escludendo che il trasferimento di un dato fra amministrazioni pubbliche modifichi la titolarità dello stesso o determini una ulteriore posizione di titolarità, delinea una soluzione diversa da quella seguita in sede di disciplina del trattamento dei dati personali (l'amministrazione che riceve dati personali da un'altra amministrazione di regola diviene a sua volta titolare del nuovo trattamento).
Articolo 60
La previsione di cui all'articolo 60, comma 1, sembra sovrapporsi, quanto a contenuto, a quella di cui all'articolo 53, comma 2. E', pertanto, necessario procedere al coordinamento delle due disposizioni, eventualmente sopprimendo una delle due.
Articolo 61
E' opportuno chiarire che i decreti di cui al commi 4 e 5, in ragione del loro contenuto, sono adottati al sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, avendo natura regolamentare.
Inoltre, malgrado il comma 6 escluda l'esistenza di oneri per la partecipazione al Comitato, l'Amministrazione dovrebbe chiarire perché ritiene che non derivino oneri di nessun tipo dall'attuazione del comma 5.

Articolo 62
In generale, occorre precisare se la realizzazione e la gestione delle basi di dati di interesse nazionale comportino oneri e, in tal caso, indicare la relativa copertura finanziaria. In proposito questo Consesso, pur prendendo atto di quanto dichiarato nella relazione tecnico-finanziaria, ritiene che la determinazione della copertura delle spese non possa essere rimessa agli atti di normazione secondaria che individueranno le singole basi di dati di interesse nazionale.
Al comma 2 va precisato il significato dell'espressione "allineamento delle informazioni".
Con riguardo al decreto di cui al comma 3, in ragione della natura regolamentare, va aggiunto che l'adozione ha luogo ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400.
15. 3 Sezione III
Articolo 64
Con riguardo alla previsione di cui al comma 1, appare necessario un richiamo anche al rispetto del principio di non discriminazione e di eguaglianza, in conformità a quanto stabilito dalla delega di cui all'articolo 10, comma 1, lettera b) della legge 29 luglio 2003, n. 229, essendovi il rischio che l'accesso al servizi prestati per via telematica sia precluso alle fasce della popolazione prive di mezzi informatici o non in grado di utilizzarli.
Il disposto del comma 3, per come è attualmente formulata la disposizione, sembra eccedente rispetto al contenuto dell'articolo 64 come indicato nella rubrica ("Organizzazione e finalità dei servizi in rete1 visto che letteralmente si riferisce a tutti i procedimenti e non solo a quelli diretti all'ammissione o comunque correlati all'erogazione di un servizio pubblico.
La previsione di cui al comma 4 va soppressa, in quando riproduce quanto già previsto dall'articolo 57, comma 1, lettera g).
Articolo 65
Occorre coordinare i commi 1 e 3, visto che il comma 1 prevede due sole modalità di identificazione informatica ai fini dell'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, ossia la carta d'identità elettronica e la carta nazionale dei servizi, mentre il comma 3 fa riferimento anche alla firma digitale.
Articolo 66
Visto che il comina 2 dell'articolo 38 del Dpr n. 445 del 2000 viene contestualmente soppresso, vorrà valutarsi l'opportunità di inserire nel citato decreto n. 445 del 2000 un richiamo alle modalità di identificazione del soggetto che presenta l'istanza o la dichiarazione previste ora dall'articolo 66 del Codice.
15. 4 Sezione IV
Articolo 67
Con riguardo alla previsione del comma 2 _giova premettere che, al sensi della vigente disciplina di cui all'articolo 36, comma 1, del Dpr n. 445 del 2000, le caratteristiche e le modalità per il rilascio della carta nazionale dei servizi devono essere definite con un decreto del Presidente del Consiglio dei Ministri, che non può, come tale, modificare o abrogare la disciplina di rango primario della materia o derogare alla stessa. In relazione a tale premessa, suscita perplessità la scelta di rimettere, con il Codice, ad un regolamento di c.d. delegificazione adottato al sensi dell'articolo 17, comma 2, della legge n. 400 del 1988 la disciplina, fra l'altro, delle caratteristiche e dell'uso della carta nazionale dei servizi; si tratta, infatti, di una materia che può incidere sulla tutela di diritti fondamentali della persona (diritto alla protezione dei dati personali, diritto alla salute e altri) e che, salva la possibilità di adottare regolamenti di esecuzione o di attuazione ai sensi del comma 1 del menzionato articolo 17, andrebbe regolata con norme di rango primario. In ogni caso, qualora si ritenga di mantenere il richiamo all'articolo 17, comma 2, della legge n. 400 del 1988, sarebbe necessario definire contestualmente nel Codice "le norme generali regolatrici della materia" come prescritto dal citato comma 2.
Il decreto previsto dal comma 6 ha natura regolamentare e va, quindi, prescritto che esso deve essere adottato secondo il procedimento previsto dall'articolo 17, comma 3, della citata legge n. 400 del 1988.
16. CAPO V
16. 1 Sezione I
Articolo 68
La previsione di cui al comma 2 va integrata, in conformità a quanto previsto dall'articolo 57, comma 6, del Dpr 21 dicembre 1999, n. 554, con la precisazione che le amministrazioni appaltanti possono porre a base di gara le proposte ideative acquisite a seguito di un concorso di idee, ma solo per le gare che abbiano ad oggetto "un concorso di progettazione ovvero di un appalto di servizi di cui ai Capi 4 e 5 del titolo 4 del citato Dpr n. 5 54 del 1999 e, comunque, solo in relazione ad appalti che ricadano nell'ambito di applicazione del suddetto decreto.

Articolo 69
Al comma 1, lettera b), occorre chiarire che si fa riferimento a programmi sviluppati per conto e a spese 'Della medesima o di altre" amministrazioni.
Il significato delle nozioni di "interoperabilità" e di "cooperazione applicativa", contenute nel comma 2, deve essere meglio precisato, se del caso utilizzando una circonlocuzione, considerato anche che manca una corrispondente definizione all'articolo I.
Articolo 70
Va definito in modo puntuale l'ambito di applicazione della previsione di cui al comma 3, dovendosi precisare se l'inserimento delle clausole ivi indicate debba avere luogo in tutte le tipologie di contratti contemplate dall'articolo 69, comma 1, che abbiano ad oggetto l'acquisizione di programmi informatici da parte dell'amministrazione, oppure - come sembra verosimile - alla sola ipotesi considerata dall'articolo 70, comma 1 (che corrisponde alla fattispecie di cui all'articolo 69, comma 1, lettera a), riferita, inoltre, ai soli programmi applicativi).
Sempre con riguardo al comma 3, anche in considerazione del rilievo innanzi formulato, l'Amministrazione riferente dovrà valutare se mantenere il riferimento alla "proprietà dei programmi ai fini del riuso" o fare ricorso ad una espressione più lata, adattabile ad una più ampia tipologia di modelli negoziali (es. "il diritto di disporre dei programmi ai fini del riuso da parte della medesima o di altre pubbliche amministrazioni").
17. CAPO VI
Articolo 72
Con riguardo al disposto del comma 1, deve essere chiarito che i decreti previsti da tale disposizione debbono essere adottati ai sensi dell'articolo 17, comma 3, della citata legge n. 400 del 1988, in considerazione della loro natura regolamentare (cfr. anche il parere della Sezione per gli atti normativi n. 7904/04 del 30 agosto 2004 reso in relazione alla "Istituzione del sistema pubblico di connettività e della rete internazionale del-la pubblica amministrazione"). Si prende atto che l'Amministrazione ha inserito nel testo l'intesa con la Conferenza unificata.
Si suggerisce, inoltre, di prevedere una verifica della coerenza tecnica di tali norme anche rispetto alle regole di cui al disciplinare tecnico pubblicato in Allegato B al D.Lgs 30 giugno 2003, n. 196.
18. CAPO VII
Articolo 74
Con riguardo al secondo periodo del comma 1, va osservato che l'obbligo di attuare i successivi interventi normativi incidenti sulla materia mediante la modifica o l'integrazione delle disposizioni del codice non si pone come vincolo per il legislatore, bensì quale precetto diretto alla Presidenza del Consiglio dei Ministri quale amministrazione competente in ordine all'adozione degli opportuni atti di indirizzo e di coordinamento. Appare, quindi, preferibile, il ricorso, con i necessari adattamenti, ad una formula analoga a quella già utilizzata all'articolo articolo 7, comma 6, della legge 8 marzo 1999, n. 50, abrogato dall'articolo 23 della legge 29 luglio 2003, n. 229 ("La Presidenza del Consiglio dei Ministri adotta gli opportuni atti di indirizzo e di coordinamento per assicurare che i successivi interventi normativi incidenti sulle materie oggetto di riordino siano attuati esclusivamente mediante la modifica o l'integrazione delle disposizioni contenute... ").
19. Per quanto concerne, infine, gli aspetti relativi alla migliore e più corretta formulazione dello schema in esame, si espongono qui di seguito ulteriori osservazioni e suggerimenti.
Il primo rilievo di ordine formale riguarda la necessità di inserire - in coerenza con quanto suggerito per gli altri codici di attuazione della legge n. 229 del 2003 - un indice delle disposizioni del codice, con la loro rubrica.
Si rileva, sempre in via preliminare, che i riferimenti normativi nelle rubriche degli articoli, effettuate nei confronti di norme da abrogare, risultano utili solo per i lavori preparatori e debbono, quindi, essere espunti nella stesura definitiva.
Si richiamano, poi, le indicazioni della "Guida per la redazione dei testi normativi", di cui alla circolare della Presidenza del Consiglio dei Ministri 2 maggio 2001, n. 1/1.1.26/10888/9.92, specie per quanto riguarda l'uso della lettera iniziale maiuscola che deve essere limitato al soli casi di uso corrente e. comunque, deve essere effettuato con criteri di uniformità. In proposito si segnala in particolare che nel testo del codice la parola "Regione" viene scritta in maniera non uniforme (v. ad es. articoli 2, comma 1, e 56, comma 2), mentre la parola "Conferenza" va scritta con l'iniziale maiuscola solo quando fa parte della denominazione di un organo, mentre deve avere l'iniziale minuscola se si designa una generica conferenza di servizi (v. articoli 9, comma 3; 37, comma 3).
L'espressione "Comunità europea" (cfr. articolo 18) va sostituita da "Unione europea" (tenendo conto che la parola "europea" va scritta con l'iniziale minuscola: v. articolo 13, comma 3).

E' opportuno modificare l'espressione "presente decreto" spesso ricorrente nel testo, con la formula "presente codice" (usata agli articoli 47, comma 3, e 51, comma 3), per accentuare il carattere proprio della normativa di cui si tratta (v. articoli 2, commi 2, 5 e 6; 3; 10, comma 6; 3 1, comma 4; 3 6; 38, comma l; 47, comma l; 63).
Dopo l'articolo 75, e fuori dalla numerazione dell'articolato, va aggiunta la clausola di inserzione del decreto nella raccolta degli atti non-nativi, del seguente tenore: "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".
Per quanto riguarda le singole parti dello schema si suggeriscono le seguenti modifiche e correzioni:
- articolo 1, comma 1, lettera s): alla penultima riga sostituire la parola "cioè" con "quale";
- articolo 2, comma 4:, penultima riga: dopo "informatici" mettere la virgola;
- articolo 6, comma 1: dopo "utilizzano" mettere la virgola;
- articolo 8: prima della parola 'facilitare" inserire "per";
- articolo 10, comma 4: sostituire "La Repubblica" con "Lo Stato";
- articolo 12, comma 1: sostituire l'espressione "a tal fine anche dettando" con "dettando anche";
- articolo 15, comma 1, lettere e) ed i): correggere l'errore materiale della ripetizione degli articoli 'la" e 'le";
- articolo 15, comma 1, lettera h) terza riga: dopo "amministrazioni" mettere la virgola;
- articolo 19, comma 2, ultima riga: dopo "interessate" mettere la virgola;
- articolo 19, comma 3: alla seconda riga, dopo "sostituiscono" mettere la virgola; alla penultima riga, dopo "appartenenza" mettere la virgola;
- articolo 24, comma 1, il riferimento all'articolo 25 è errato (controllare se si tratta invece dell'articolo 23), cosi come avviene per una serie di indicazioni successive, che vanno tutte accuratamente verificate (v. articolo 25, comma 3, lettera b), che dovrebbe riferirsi all'articolo 27, comma 3; articolo 26, comma 2, che dovrebbe riferirsi all'articolo 23, comma l; articolo 27, comma 1, lettera d), che dovrebbe riferirsi all'articolo 29; articolo 3 1, comma 1, lettera a), che dovrebbe riferirsi all'articolo 26; articolo 34, comma 4, che dovrebbe riferirsi all'articolo 26, comma 6; articolo 42, comma 4, che dovrebbe riferirsi all'articolo 45; articolo 57, comma 1, lettera g), che dovrebbe riferirsi all'articolo 64, comma 4; articolo 63, comma 1, che dovrebbe riferirsi al comma 3 dell'articolo richiamato);
articolo 37, comma 3: il riferimento agli articoli "14 e seguenti" della legge n. 241 del 1990 va precisato nel riferimento agli articoli "da 14 a 14-quinquies" della stessa legge, nel testo recentemente innovato con legge approvata in via definitiva dalla Camera dei Deputati il 26 gennaio 2005 e in attesa di promulgazione;
- articolo 38, comma 2: correggere l'errore materiale "uve" = "ove";
- articolo 41, comma 3, ultime due righe: dopo "omogenea" mettere la virgola e toglierla dopo la parola "progressiva";
- articolo 44, comma 2: dopo "conservare" mettere la virgola;
- articolo 54, comma 1: alla fine mettere il segno del punto;
- articolo 54, comma 2: le parole "custodite" e "controllate" debbono essere volte al maschile concordando con "documenti";
- articolo 57, comma 1, lettera c): "8 agosto"= '7 agosto"; lettera a): indicare gli estremi dei Dpr;
- articolo 62, comma 4: tra le parole "articolo" e "decreto" inserire "8 del";
- articolo 63, l'aggettivo "previsto" va eliminato,
- articolo 66, al comma 1 dopo le parole "articolo 38" occorre aggiungere, dopo la virgola, le parole "commi 1 e 3"; articolo 67, comma 1, terza riga, e comma 4, seconda riga: dopo "anno" aggiungere "di età"; articolo 67, comma 2: l'espressione "dell'articolo Il 7, sesto comma, della Costituzione" appare superflua e può essere espunta;
- articolo 67, comma 4, dopo l'entrata in vigore del citato D.Lgs n. 196 del 2003, è opportuno sostituire la parola "riservatezza" con le parole "protezione dei dati personali";
- articolo 67, comma 5, penultima riga: dopo "articolo 72" mettere la virgola; inoltre le parole "ai sensi dell'articolo" vanno sostituite con le parole "di cui all'articolo";
- articolo 67, comma 6, terza riga: correggere "articolo 9" in "articolo 8";
- articolo 72, comma 1, quarta riga: correggere "articolo 9" in "articolo 8".

PQM

Esprime parere favorevole con le suesposte osservazioni.

Quando le norme vengono scritte male: finalmente chiarezza sul Codice della Pubblica Amministrazione Digitale

di Andrea Lisi (Avvocato, www.studiodl.it)

In vari articoli ho espresso numerosi dubbi sulla qualità delle ultime "rivoluzioni" in materia di documento informatico (e anche di posta elettronica certificata); dubbi alimentati anche dal fatto che si considerano certe e si pongono in essere "campagne stampa" su normative che sono ancora in fieri, costituendo ancora degli "Schemi di Decreto".
In maniera libera e disinteressata alcuni giuristi in Italia, tra i quali il sottoscritto, si sono permessi di sottolineare i pericoli di certe normative così rigide per il futuro del commercio elettronico e hanno espresso le proprie forti perplessità in merito a "schemi di legislazione" che sembravano percorrere una strada assurda, difficile, contorta, "monopolista", a tutto danno della libertà dell'Internet e del documento informatico.
Ebbene, in un articolato parere (parere 11995/05 reso nell'Adunanza del 7 febbraio scorso) il Consiglio di Stato ha pesantemente criticato il Codice della Pubblica Amministrazione Digitale (Schema di Decreto Legislativo) ribadendo, in maniera autorevole, come certe normative vadano riconsiderate in maniera più meditata e, quindi, vadano redatte con maggiore attenzione.
Il parere del Consiglio di Stato conferma tutte le critiche manifestate in questi mesi e, in particolare, accredita autorevolmente l'opinione di chi ha affermato:
- che non avesse senso "gettare all'aria" tutta la normativa passata (tra l'altro il D. Lgs. n. 10 del 2002 di recepimento della direttiva 1999/93/CE era entrato in vigore neppure tre anni fa e aveva già operato una semplificazione in materia di documento informatico!)
- che certe normative andavano meditate maggiormenete, anche con l'aiuto di giuristi, e che sembravano scritte più da tecnici che da esperti del diritto
- che era indispensabile garantire la sopravvivenza del documento informatico scritto, "firmato", non sottoscritto (ossia di quel documento informatico in qualsiasi modo "associabile" ad un soggetto giuridico) per il futuro del commercio elettronico tra privati
- che non si dovesse legare l'evoluzione del documento informatico alla sola firma digitale, ma si dovesse garantire l'evoluzione tecnologica e la prassi fatta di tante possibili forme di firme elettroniche (come anche sottolineato dalla direttiva 1999/93/CE)
- che fosse un'assurdità giuridica (oltre che un pericolo per la validità di tutte le transazioni telematiche) associare la "forma scritta" al solo documento informatico munito di firma digitale
- che dall'esame di alcune norme del Codice si potessero ravvisare profili di incostituzionalità nello stesso Codice
Per tutte queste ed altre ragioni abbiamo manifestato forti perplessità su questo Schema di Decreto, salutato da alcuni come la "nuova rivoluzione digitale" o la panacea per tutti tutti i mali della precedente normativa.
Oggi un autorevole, articolato parere "bacchetta" quello schema di normativa "frettolosa" e infelice in molti suoi aspetti, consigliando ai suoi redattori di andare a studiare con calma "le indicazioni della Guida per la redazione dei testi normativi, di cui alla Circolare della Presidenza del Consiglio dei Ministri 2 maggio 2001, n. 1/1.1.26/10888/9.92"!
In particolare e in estrema sintesi, il parere del Consiglio di Stato (del quale si consiglia la attenta lettura) analizza punto per punto le norme del Codice, criticandone numerosi aspetti (anche stilistici) e chiedendo che vengano acquisiti i pareri di altre amministrazioni (oltre al ministero dell'Economia, devono essere ascoltati anche il dipartimento della Funzione pubblica e i dicasteri dell'Interno e della Giustizia) su alcuni punti problematici che si provano a riassumere:
- il Codice è pieno zeppo di "enunciazioni programmatiche e di principio, contenute in varie parti del testo", ma alle stesse devono essere affiancate "norme precettive - applicabili tramite un processo graduale e guidato di implementazione o, in altri casi, direttamente esecutive"
- il testo viene, inoltre, censurato per la mancata previsione di risorse finanziarie adeguate per sostenere questo cambiamento.
- è necessario che il nuovo Codice nell'accelerare il cambiamento, prevenga con misure concrete l'incremento del fenomeno del "digital divide"
- è ancora indispensabile che il testo tenga in maggiore considerazione le esigenze di raccordo con le reti regionali e locali
Ma le critiche più pesanti e impietose vengono manifestate lungo l'analisi delle singole norme del Codice; analisi che viene effettuata con puntigliosa attenzione. E, come vedremo, numerose

considerazioni critiche vengono espresse proprio sugli articoli 17 e 18 relativi al valore formale e probatorio del documento informatico.
Alla luce di queste premesse, il Consiglio di Stato "considerata la natura strutturale di talune delle osservazioni del presente parere e ritenuto che svariate tra esse debbano essere risolte con la partecipazione delle amministrazioni richiamate, ma constatate altresì la prossimità della scadenza del termine della delega e l'impossibilità di rispettarlo laddove si dovesse procedere ad approfondimenti istruttori, suggerisce sin d'ora di valutare l'eventualità di stabilire un congruo termine per l'entrata in vigore dello schema in oggetto (ad esempio, 180 o 240 giorni). Ciò consentirebbe, oltre che di preparare adeguatamente le amministrazioni e gli operatori ai cambiamenti introdotti, di predisporre la raccolta di norme regolamentari di cui si dirà infra, al punto 9, nonché di far confluire le modificazioni che eventualmente non vi fosse stata la possibilità di apportare con il necessario approfondimento in uno o più decreti legislativi correttivi, consentiti dall'articolo 10, comma 3, della legge 229/03".... insomma un Codice che nel momento in cui dovesse entrare in vigore già dovrà essere pesantemente modificato e corretto da altri decreti legislativi che verranno!!!
Lungo il suo parere il Consiglio ha espresso numerose meditate critiche delle quali si ricorda l'importante monito: "la presenza di nuovi mezzi di svolgimento dell'attività amministrativa impone, quando le innovazioni lo consentono, il compimento di operazioni di adattamento dei vecchi istituti alle nuove situazioni (si ricordi l'insegnamento di "interrogare i nuovi ordinamenti adoperando gli antichi istituti e modificandoli, quando necessario")". O ancora l'inquietante considerazione che "appare, anzi, quantomeno singolare che la norma sulle abrogazioni (articolo 75) si incentri come si è detto esclusivamente sul D.Lgs 10/02 e sul Tu 445/00, cosi concentrando (e limitando) la propria opera di "riassetto" su una normativa che in realtà era stata già riordinata di recente, tralasciando invece tutte le altre norme sulla materia, presenti, spesso in modo asistematico, in molteplici fonti dell'ordinamento".
Dovrebbe far riflettere, inoltre, la considerazione che "appare limitativo volere codificare la fase attuale (fermatasi, allo stato della tecnica, alla firma digitale, di cui la dottrina afferma la artificiosità), mentre in un futuro, forse anche imminente, potrebbero raggiungersi diverse e più efficaci modalità di esternazione degli atti o di apposizione di sigilli, etc. (si pensi alla impronta del dito, alla identificazione attraverso l'iride, alla certezza del dna per la identità dei soggetti, alla videoconferenza certificata). E quindi " sempre a titolo di esempio, si rileva come la sicurezza sulla firma digitale appaia, allo stato, temporanea, con la conseguente necessità di modificare la chiave privata piuttosto frequentemente. Risultano, però, allo studio sistemi più sicuri (quali impronte digitali, impronte retiniche, etc.). Ciò dovrebbe indurre a rendere più flessibili le relative previsioni (anche laddove se ne evitasse la criticata "legificazione"): dovrebbe, pertanto, valutarsi l'opportunità di inserire fin d'ora previsioni che limitino la normativa introdotta fino al momento in cui sarà tecnicamente possibile imprimere agli atti e ai documenti informatici impronte antropometriche (o, in ogni caso, sistemi più sicuri di quelli ora previsti), che consentano senza possibilità di errore di stabilire la provenienza, la firma, etc.".E ancora " Occorre osservare che la Direttiva comunitaria n. 1999/93/CE, che ha introdotto un quadro comunitario per le firme elettroniche, distingue (articolo 2, dedicato alle definizioni) la "firma elettronica" dalla "firma elettronica avanzata". Anche in considerazione della normativa comunitaria, particolari problemi presenta la distinzione (la graduazione, come si precisa nelle legge di delega) tra i vani generi di firma, ovvero tra le lettere r), s), e t) dell'articolo. (...) Sembra quindi inopportuna la distinzione apparente in tre diverse specie di firma e, se deve essere apprezzata la riduzione a tre delle ipotesi di firma (sono quattro nell'attuale Dpr n. 445 del 2000), sarebbe opportuno un ulteriore chiarimento, nel senso che i tipi di firma sono solo due, la firma elettronica pura e semplice e quella qualificata, di cui la firma digitale è un tipo".
Ed è proprio sugli aspetti del valore formale e probatorio del documento informatico che la critica si fa impietosa e senza appello!
Prima di tutto il Consiglio di Stato sottolinea che per la redazione del testo definitivo risulta necessario e indispensabile quanto meno l'avviso motivato del "Ministero della giustizia su alcune questioni di rilievo, di seguito individuate, e segnatamente su quelle che incidono sulla rilevanza probatoria dei documenti, sull'ordinamento civile con particolare riguardo al rapporti tra privati (articoli 17 e 18)."
Si riportano, per concludere, alcune considerazioni contenute nel parere del Consiglio sugli articoli 17 e 18 che dovrebbero portare tutti a riflettere su quanto "sbandierato" in questi giorni in merito al valore formale e probatorio dei documenti scritti, firmati non sottoscritti (quali anche le semplici e-mail):
- Ben avrebbe potuto il legislatore "introdurre la forma della scrittura telematica, munita o meno di una firma sicura -o più o meno sicura, ritenendola idonea al perseguimento degli scopi di legge. Basti pensare che il D.Lgs 50/1993, sui contratti a distanza, prevede "contratti conclusi mediante l'uso di

strumenti informatici e telematici", con la ulteriore possibilità di distinguere, anche per lo strumento utilizzato, le scritture (non sottoscritte) da quelle sottoscritte, asseverate dalla sottoscrizione"
- "A prescindere dall'antico dibattito dottrinale sulla distinzione tra atto e documento, non si può sottacere che una cosa è il documento, che è il contenente (che è un mezzo di prova), altra cosa è il contenuto o l'atto documentato (il negozio o atto giuridico voluto), altra cosa ancora è la forma, che è elemento essenziale dell'atto o negozio, se prescritta a pena di nullità (articolo 1325 c.c.) e che può consistere nell'atto pubblico o nella scrittura privata, autenticata o non (v. articolo 1350 c.c.). La affermazione, contenuta nello schema di codice, che sia il documento informatico (sottoscritto con firma digitale) a soddisfare il requisito della forma scritta sembra invece confondere il contenente con il contenuto."
- "Minori problemi in materia crea il vigente articolo 10 del Dpr n. 445 del 2000, che per il documento informatico in sé, a prescindere dalla sottoscrizione, rinvia all'articolo 2712 c.c. e prevede (comma 2) che il documento informatico sottoscritto con firma elettronica soddisfa il requisito della forma scritta, dandosi cosi carico di attribuire un valore a qualsiasi documento informatico, a prescindere dalla forza della firma"
- "Peraltro, l'idoneità della forma a conseguire un effetto si desume, secondo la dottrina, dall'articolo 121 c.p.c., sulla strumentalità (idoneità allo scopo) delle forme. Si dovrebbe pertanto cercare di affrontare anche nel nuovo codice il tema del valore dell'atto adottato con scrittura telematica anche ove non sia munito di sottoscrizione, laddove sia conosciuto l'autore per la provenienza dal suo indirizzo elettronico, ovvero ove sia sottoscritto con firma elettronica c.d. debole"
- "Gli articoli 17 e 18 non chiariscono se sia idonea forma scritta, a tal fine, ai sensi dell'articolo 1350 c.c., la scrittura con firma soltanto elettronica. Anzi, l'articolo 18 sembra escludere tale possibilità, in quanto il secondo comma prevede il soddisfacimento della forma scritta solo per il documento (non per l'atto) con firma elettronica qualificata o firma digitale. Ne discende che la scrittura con firma elettronica (non qualificata) non sembrerebbe integrare la scrittura privata non autenticata di cui all'articolo 1350 c.c., anche se gli autori della scrittura non disconoscono la loro firma. Non si comprende come debba essere considerato l'atto con firma elettronica debole non disconosciuta a norma dell'articolo 215 c.p.c. La previsione della libera valutabilità in giudizio, di cui al primo comma dell'articolo 18, sembra contrastare con il principio desumibile dal codice di rito".
Più chiaro di così.....
18/02/2005

Parte II

PARTE II

INFORMATICA

Questa seconda parte del volume è divisa nei seguenti capitoli: "nomi di dominio", "processo telematico" e "reati informatici".

Per quanto riguarda il primo capitolo di particolare interesse è la prima scheda che riporta integralmente un articolo di R. Manno sui rapporti fra nomi a dominio e proprietà industriale.

Segue la trattazione della tematica del processo telematico .

Nel terzo capitolo, infine, è stata approfondita l'evoluzione normativa che ha condotto l'Italia a introdurre una disciplina integrativa del codice penale, la l. n. 547/1993, volta a qualificare come reati alcune condotte poste in essere attraverso tecnologie informatiche e telematiche.

In particolare nel nostro Paese i giuristi hanno osservato il principio del "nullum crimen sine lege" senza per questo rinunciare alla sanzione di condotte criminose largamente dannose per privati ed enti pubblici.

Sono state anche adottate leggi speciali che hanno previsto nuove ipotesi delittuose.

INFORMATICA

CAPITOLO I

NOMI DI DOMINIO

Il 1 marzo 2002 è divenuto operativo il nuovo Istituto di Informatica e Telematica (IIT) del CNR, nato dalla fusione dell'Istituto per le Applicazioni Telematiche con l'Istituto di Matematica Computazionale.

L'Istituto di Informatica e Telematica (il cui sito è: http://www.iit.cnr.it), con sede a Pisa, svolge la funzione di Registro del ccTLD[1] ".it", responsabile dell'assegnazione dei nomi a dominio all'interno del country code top level domain ".it" (ISO 3166) e gestisce quindi i registri operativi dei domini con estensione "IT".

ccTLD e' infatti un acronimo per "country code Top Level Domain" ossia l'estensione del dominio (.it/fr/de/es...) associata ad ogni nazione (Italia/Francia/Germania/Spagna...).

Questo ruolo è stato riconosciuto da IANA (Internet Assigned Numbers Authority) fino dal 1987 e successivamente da ICANN (The Internet Corporation for Assigned Names and Numbers).

Il NIC italiano (Registro per il ccTLD "it") è raggiungibile all'indirizzo http://www.nic.it/.

La registrazione dei nomi a dominio sotto il country code Top Level Domain "it" avviene sulla base del Regolamento e delle procedure tecniche di registrazione

L'Istituto di Informatica e Telematica interagisce con oltre 2000 provider/maintainer. I nomi a dominio registrati attualmente nel ccTLD "it" sono oltre 700 mila

Per dominio si intende un insieme di simboli alfanumerici (nome), così come definito dalle singole Authority, capace di associarsi in maniera univoca ad un Domain Name System (DNS).

---

[1] *ccTLD e' un acronimo per "country code Top Level Domain" ossia l'estensione del dominio (.it/fr/de/es...) associata ad ogni nazione (Italia/Francia/Germania/Spagna...).*

I computer collegati a Internet comunicano tra loro per mezzo di un "protocollo Internet" e sono contrassegnati da un indirizzo IP o numero IP (per esempio 193.60.233.1) assegnato dall'ISP (Internet Service Provider).

Poiché è difficile ricordarsi tutti questi numeri, è stato ideato il "Domain Name System" (DNS) grazie al quale l'utente di Internet può inserire parole o nomi. Un nome a dominio corrisponde anche a un indirizzo Internet.

Un nome a dominio può essere formato solo da numeri e lettere e deve essere unico. Nel caso in cui, successivamente alla registrazione, sia necessaria una modificazione è necessario, in via preliminare, provvedere alla sua cancellazione e alla conseguente registrazione del un nuovo nome a dominio.

La registrazione di un nome a dominio è consigliata a tutti coloro che vogliono essere raggiungibili tramite una home page su Internet.

A grandi linee, la procedura e gli organismi preposti alle procedure di regolamentazione, assegnazione e registrazione dei nomi di dominio in Italia sono due:

- *la autorità italiana di registrazione, attualmente l'Istituto di Informatica e telematica di cui si è parlato prima, si occupa dell'assegnazione e registrazione vera e propria di tutti i nomi a dominio compresi nel suffisso '.it'.*
- *la Naming Authority Italiana, si occupa di stabilire le regole e le procedure con cui gestire i domini. Una delle regole principali è quella dell'unicità del dominio, ovvero una volta assegnato un certo nome di dominio, nessun altro potrà più usufruirne. Altra regola definisce che l'assegnazione avvenga secondo il criterio di priorità temporale, senza verificare prima l'eventuale conflittualità con altri marchi registrati.*

L'individuazione giuridica dei domain name resta una delle problematiche principali del diritto delle tecnologie informatiche.

NUMERO SCHEDA: 6297

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: NOMI DI DOMINIO

FONTE: INTERLEX

AUTORE: Roberto Manno

NATURA ATTO: COMMENTO

DATA ATTO: 18/05/

La teoria attualmente più diffusa annovera i *domain name* fra i segni distintivi atipici. Ciò verrebbe confermato sia a livello giurisprudenziale (in particolare sent. Tribunale di Modena 1571/2004), sia a livello normativo. In proposito l'art. 22 del codice della proprietà industriale, recentemente entrato in vigore, vieta l'adozione o l'uso di un nome a dominio aziendale uguale o simile all'altrui marchio.
Nel commento qui di seguito allegato si contesta questa impostazione anche sulla base della posizione assunta dalla Wipo, massima organizzazione in materia di proprietà industriale che non ha mai avallato una definizione giuridica di *domain name* in termini di segni distintivi.
L'ostacolo maggiore alla qualificazione giuridica del nome a dominio come segno distintivo è l'assenza in esso del requisito della capacità distintiva, senza la quale il segno distintivo non può essere tale.
Si allega il commento.

Si segnala inoltre una ricca sezione sulla materia dei nomi a dominio sul sito: *http://www.interlex.it/nomiadom/indice.htm*

Nomi a dominio, un problema ancora aperto

di Roberto Manno* - 18.05.05

A distanza di dieci anni, l'individuazione di una disciplina giuridica uniforme in materia di *domain name* resta ancora una delle principali problematiche del diritto delle tecnologie informatiche. Chi legge gli articoli di questa rivista ben saprà come i *domain name*, costituendo il passaggio obbligato per ogni genere di attività on-line, assumono importanza fondamentale nel cd. diritto delle nuove tecnologie.
L'introduzione del dominio generico ".eu", insieme ai nuovi domini tematici ".job" e ".travel", confermano ancora una volta la rilevanza internazionale della questione, vale a dire la natura giuridica dei *domain name*.
La teoria più diffusa attualmente annovera i *domain name* tra i segni distintivi atipici. Ciò, oltre che in numerose sentenze, tra cui la rilevantissima sentenza del tribunale di Modena n. 1571/2004, troverebbe conferma nel codice sulla proprietà industriale (c.p.i.) recentemente entrato in vigore.

L'art. 22 c.p.i. vieta infatti l'adozione o l'uso di un nome a dominio aziendale uguale o simile all'altrui marchio.
Posta la pacifica applicabilità al *domain name*, in certe situazioni, della disciplina sulla concorrenza e sulla tutela delle privative industriali, si avanzano al contrario seri dubbi sul fatto che il *domain name*, in quanto tale, costituisca una species atipica della famiglia dei segni distintivi.
Una tale qualificazione *business oriented* del *domain name*, e più in generale dell'internet, non tiene in debito conto la pluralità delle attività che possono condursi on line ed è inoltre incompatibile con i principi genetici dei diritti di proprietà industriale (tra cui appunto i segni distintivi) che non potrebbero trovare applicazione on line.
Non è un caso, dunque, che alcuni tra i più illuminati autori abbiano formulato teorie molto più aderenti alla natura tecnologica del *domain name*: ci si riferisce alla teoria di Patrizio Menchetti che, leggendo attentamente le norme del settore delle telecomunicazioni, disciplinato in Italia dalla legge 249/97, dal D.P.R. 318/97 e dalla delibera n.6/00/CIR dell'Autorità per le garanzie nelle comunicazioni, intravede nel *domain name* una "risorsa di numerazione atipica" (http://www.lc.camcom.it/marchi.pdf).
La versatilità della teoria della numerazione atipica, inoltre, non osta alla applicazione delle norme a tutela non solo dei diritti di marchio, ma anche di tutti i numerosi diritti e situazioni giuridiche con i quali il *domain name* può interferire.
La massima organizzazione in materia di proprietà intellettuale, la Wipo, da tempo segue attentamente l'evoluzione dei *domain name* cercando di offrire soluzioni alle interferenze più evidenti tra questi e i diritti di proprietà industriale. Il secondo rapporto della Wipo è dedicato proprio alle ipotesi di interferenza tra i *domain name* e denominazioni diverse dai segni distintivi di natura industriale.
La Wipo non ha mai avallato una definizione della natura giuridica del *domain name* in termini di segni distintivi.
Ritornando all'ottima sentenza del tribunale di Modena, rileviamo come in essa siano affermati importanti principi:
1) la rilevanza del *domain name* (in senso lato) sotto il profilo dei diritti di proprietà industriale per la sua funzione tipica distintiva, simile a quella svolta dall'insegna;
2) la conseguente applicabilità, in virtù dell'unitarietà dei segni distintivi, delle relative norme (tra cui l'ex art. 18 l.m.);
3) la dilatazione del presupposto del rapporto di concorrenzialità ai fini dell'applicazione dell'art. 2598 c.c.. Il *domain name* infatti coprirebbe un raggio talmente ampio di attività da porre chiunque lo detenga in posizione di diretta concorrenza con tutti coloro che svolgono, direttamente o indirettamente, attività connesse al significato di tale *domain name*.
Ora, per ammettere tale qualificazione, si dovrebbe affermare che anche il *domain name*, come tutti i segni distintivi, debba possedere il requisito della capacità distintiva, senza il quale un segno distintivo non può dirsi tale.
Tuttavia questo è impossibile: si pensi ai domini generici, coincidenti con parole di significato comune. Inoltre, i *domain name* rendono impossibile l'applicazione degli ulteriori e fondamentali principi di territorialità (si pensi ai domini .com) e di specialità (il dominio è in posizione di assoluta astrazione rispetto ai servizi e prodotti offerti, ammesso che sia utilizzato a scopi imprenditoriali).
E' proprio la conseguenza pratica di tale qualificazione a determinare un'insanabile contraddizione con i principi cardine del diritto industriale: si pensi infatti ad una denominazione di uso comune. Mentre nel mondo fisico una tale denominazione darebbe luogo ad un segno distintivo che non troverebbe cittadinanza giuridica in quanto sprovvisto di capacità distintiva (gli specialisti del diritto industriale conoscono bene il fenomeno della volgarizzazione del marchio), nel mondo virtuale vaste situazioni di monopolio si troverebbero collegate ad un tale segno distintivo… sprovvisto della minima capacità distintiva.
Con ciò non si intende mettere in discussione le conclusioni cui perviene il giudice di Modena in materia del cosiddetto "cybersquatting". Questo, quando riguardi un *domain name* corrispondente ad una denominazione di uso comune, non è idoneo a ledere alcun diritto anteriore, non potendo quindi essere ritenuto illecito.Tuttavia, riconoscendo al *domain name* la natura giuridica di segno distintivo, ciò non potrebbe più essere sostenuto.
Emerge così una delle più profonde differenze tra i segni distintivi (tipici e atipici) e i *domain name*s: nonostante i numerosi punti di contatto tra i primi e i secondi sono proprio tali differenze a ricordarci come in realtà si tratta di risorse distanti tra loro anni luce.
È per tali ragioni che, tempo fa, parlavamo provocatoriamente dei *domain name* come di qualcosa "oltre" il marchio.

Le disposizioni del c.p.i. non influiscono su queste considerazioni: esse prevedono, componendole, alcune ipotesi di interferenza tra il *domain name* e i diritti di proprietà industriale. Tra queste può rientrare anche l'uso e la registrazione di un nome a dominio "aziendale" identico o simile al marchio. Tuttavia le norme del c.p.i. fanno riferimento ad ipotesi compatibili con le norme esistenti che non possono essere lette come una qualificazione giuridica del *domain name*.
Il ricorso ai principi del diritto industriale per la qualificazione giuridica dei *domain name* rischia, inoltre, di operare una lettura in termini commerciali o imprenditoriali dell'intera rete internet, che invece è la sede dove fondamentali diritti e interessi possono e debbono trovare piena attuazione e tutela.

E' stata pubblicata la direttiva "Conoscenza ed uso del dominio internet "gov.it" ed efficace interazione del portale nazionale "italia.gov.it" con le pubbliche amministrazioni e le loro diramazioni territoriali.

NUMERO SCHEDA: 1639

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: NOMI DI DOMINIO

FONTE: GAZZETTA UFFICIALE

DATA: 11/07/2002

RIFERIMENTO NORMATIVO: art. 5 legge 400/88; art. 3 legge 20/94

NATURA ATTO: DIRETTIVA

DATA ATTO: 30/05/2002

ORGANO: CONSIGLIO DEI MINISTRI

Sulla Gazzetta Ufficiale dell'11 luglio 2002 n. 161 è stata pubblicata la direttiva del Presidente del Consiglio dei ministri 30 maggio 2002 "Conoscenza ed uso del dominio Internet gov.it ed efficace interazione del portale nazionale italia.gov.it con le pubbliche amministrazioni e le loro diramazioni territoriali". La direttiva è rivolta alle amministrazioni centrali dello stato ed agli enti pubblici sottoposti alla vigilanza dei ministeri e si riferisce a tutte le amministrazioni che offrono servizi pubblici di tipo conoscitivo ai cittadini ed alle imprese. Per le regioni e gli enti locali "costituisce contributo alle determinazioni in materia, nel rispetto della loro autonomia", per le altre pubbliche amministrazioni costituisce uno "schema di riferimento".
Le pubbliche amministrazioni destinatarie della direttiva devono operare in modo da garantire che entro il 2005 tutti i servizi più importanti siano offerti in formato elettronico. Inoltre i siti dovranno garantire il riconoscimento dell'utente e l'accesso ai servizi mediante la carta d'identità elettronica e la carta nazionale dei servizi e la possibilità di accettare le istanze inviate in via telematica. Dovranno inoltre indicare le istanze e le dichiarazioni che richiedono la firma digitale e quelle per le quali, non essendo necessaria la sottoscrizione, basta l'identificazione con la carta d'identità elettronica. Il passaggio a tale modalità di accesso deve essere realizzato non subito, ma gradualmente e contestualmente alla diffusione di tali strumenti, per cui attualmente si può continuare con i sistemi di identificazione ordinari.

La direttiva per la conoscenza e l'uso del dominio gov.it fissa dunque un insieme di requisiti di qualità: l'obiettivo è quello di aggregare i siti ed i portali delle Amministrazioni statali che erogano servizi istituzionali con un adeguato ed omogeneo livello di qualità, sicurezza ed aggiornamento dei servizi stessi. Le amministrazioni sono chiamate a porre in atto azioni di autovalutazione dei propri siti per definire eventuali interventi di adeguamento. Il Cnipa cura la promozione dell'iniziativa e il monitoraggio della direttiva.
La modalità di assegnazione dei nomi nel dominio ".gov.it" è analoga a quanto ad oggi avviene per la registrazione di nomi nel dominio ".it" o sotto la sua struttura geografica predefinita. La procedura di registrazione prevede l'invio - da parte del richiedente - di una lettera di assunzione di responsabilità dell'uso del dominio stesso. Ogni altra attività relativa alla gestione dei domini, come cambio di nome, cessazione, riassegnazione, cambio di provider/mantainer, modifica della delega ecc. deve essere tempestivamente comunicata al Cnipa.

Si allega il testo.

Dir.P.C.M. 30 maggio 2002 (1).
Conoscenza ed uso del dominio internet «.gov.it» ed efficace interazione del portale nazionale «italia.gov.it» con le pubbliche amministrazioni e le loro diramazioni territoriali.

1. *Premessa.*
Nel processo di continua trasformazione delle pubbliche amministrazioni italiane, l'innovazione tecnologica rappresenta un fattore di sviluppo e di razionalizzazione, oltre che di risparmio della spesa pubblica e, soprattutto, di miglioramento dei servizi resi al cittadino-utente ed alle imprese.
Per consentire un cambiamento concreto ed effettivo è indispensabile, da un lato, disporre di nuovi sistemi di servizio al cittadino ed alle imprese; dall'altro, realizzare un'efficace azione di coordinamento, sia sul piano amministrativo-organizzativo che su quello tecnico-informatico, anche mediante l'adozione di direttive ed indirizzi in materia.
In questa prospettiva di cambiamento il Ministro per l'innovazione e le tecnologie ha reso attivo e registrato il dominio di secondo livello «.gov.it». È stato altresì realizzato il portale nazionale per il cittadino ed analoga iniziativa è in corso per le imprese.
L'obiettivo del dominio è quello di aggregare i siti ed i portali delle amministrazioni statali che già erogano e che erogheranno servizi istituzionali con un adeguato ed omogeneo livello di qualità, sicurezza ed aggiornamento dei servizi stessi.
La necessità di rendere omogenei i servizi offerti comporta che l'iscrizione al dominio verrà condizionata ad alcuni criteri essenziali finalizzati ad assicurare le caratteristiche predette. Analogamente il portale nazionale consentirà agli utenti un agevole accesso ai servizi erogati dalla pubblica amministrazione in modo omogeneo, aggregato e completo.
2. *Caratteristiche generali dei siti.*
I siti facenti parte del dominio «.gov.it» hanno lo scopo di fornire informazioni e servizi ai cittadini, alle imprese e alla stessa pubblica amministrazione con la garanzia per questi che le informazioni ed i servizi richiesti provengano direttamente dall'ente e abbiano le caratteristiche di qualità di seguito indicate. Tali siti devono contenere informazioni e servizi chiaramente presentati, raggruppati in modo organico per gli utenti e facilmente raggiungibili dalla pagina web principale.
2.1. *Definizione del nome di dominio.*
Le regole di definizione dei nomi di dominio attuali hanno impedito il ricorso ad una uniforme denominazione dei siti.
I nomi di dominio di terzo livello da utilizzare nell'àmbito del dominio «.gov.it» dovranno essere il più possibile autoesplicativi e brevi; a tal fine è opportuno non inserire nel nome il suffisso «ministero, ente, dipartimento ...» (es. innovazione.gov.it).
2.2. *Accessibilità.*
La presentazione delle informazioni e dei servizi deve garantire l'utilizzo universale, quindi tutti i siti devono essere conformi al livello A di accessibilità previsto dal WAI del consorzio W3C, così come ribadito nella comunicazione della Commissione europea del 25 settembre 2001 («Accessibilità dei siti

internet pubblici e loro contenuti»), e alla *circolare del 6 settembre 2001, n. AIPA/CR/32* «Criteri e strumenti per migliorare l'accessibilità dei siti web e delle applicazioni informatiche a persone disabili».
2.3. *Usabilità.*
La rispondenza alle raccomandazioni WAI non assicura che il sito sia «usabile».
L'usabilità implica che il sito sia facilmente navigabile, e strutturato in modo tale da permettere al navigatore di reperire facilmente le informazioni richieste. Ad esempio, la struttura deve prevedere una barra di navigazione ripetuta in tutte le pagine interne del sito, e una intestazione in cui evidenziare le principali voci di riferimento e facilitare la ricerca. La presenza di un motore di ricerca nel caso di siti complessi e strutturati su un numero rilevante di pagine è auspicabile. I formati dei testi devono permettere la lettura attraverso i principali motori di ricerca, per quanto possibile anche nelle versioni meno recenti.
2.4. *L'efficacia.*
I contenuti dei siti devono essere esaustivi e aggiornati continuamente. Devono essere chiari e affidabili e i servizi offerti in linea efficienti e in grado di garantire il più possibile il completamento della pratica amministrativa. Le amministrazioni destinatarie della direttiva devono operare in modo da garantire che entro il 2005 tutti i servizi più importanti siano offerti in formato elettronico. Le aspettative degli utenti devono essere soddisfatte: i nuovi contenuti devono essere messi in evidenza in modo da essere facilmente reperiti. Un minimo di informazioni relative alla struttura organizzativa dell'amministrazione pubblica, alla sua composizione, nonché riferimenti relativi alle persone responsabili dei diversi settori (indirizzo di posta elettronica) devono essere previsti, nonché i comunicati stampa relativi all'attività dell'amministrazione. Devono inoltre essere previsti spazi di efficace interazione con i cittadini (ad esempio, i forum di discussione, se presenti, devono essere moderati). Questo peraltro non deve rappresentare il contenuto principale del sito, che deve essere focalizzato sulla erogazione di servizi all'utente.
2.5. *Identificazione e controllo di accesso.*
I siti dovranno garantire il riconoscimento dell'utente e l'accesso ai servizi mediante la carta d'identità elettronica e la carta nazionale dei servizi. La disponibilità di questa tipologia di identificazione e controllo di accesso deve essere compatibile con la diffusione di questi strumenti ai cittadini: pertanto in via transitoria è possibile conservare le modalità di identificazione attualmente in uso.
Devono essere previsti meccanismi di accettazione delle dichiarazioni e delle istanze inviate per via telematica (art. 9 del *decreto legislativo 23 gennaio 2002, n. 10*.) A tal fine devono essere indicate le istanze e le dichiarazioni che richiedono la sottoscrizione mediante firma digitale, basata su di un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura e quelle per le quali, non essendo necessaria la sottoscrizione, è sufficiente l'identificazione dell'autore da parte del sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi.
2.6. *Privacy e sicurezza.*
Al fine di proteggere e tutelare efficacemente le informazioni e i servizi in linea dei siti è necessario applicare ad essi adeguate misure di tutela della privacy e di sicurezza. I siti che offrono servizi interattivi e/o dispongono di basi di dati personali (ad esempio, liste di indirizzi di posta elettronica relativi a servizi informativi) devono essere conformi a quanto previsto dalla *legge 31 dicembre 1996, n. 675*, e successive modifiche («Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»). Inoltre, in base a quanto previsto dalla direttiva del Presidente del Consiglio dei Ministri 16 gennaio 2002 («Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni statali»), i siti devono beneficiare, in tempi brevi, di tutte le attività tecniche ed organizzative necessarie al fine del raggiungimento della «base minima di sicurezza» prevista dalla direttiva. I siti che espongono servizi di particolare criticità (ad esempio pagamenti in linea, scambi di dati sensibili, ecc.) devono garantire ulteriori misure di sicurezza finalizzate alla protezione della rete, dell'infrastruttura logica e fisica del sito.
2.7. *Monitoraggio.*
Devono essere previsti sistemi o procedure di monitoraggio interno al fine di valutare periodicamente l'utilizzo e l'efficienza dei servizi ed il grado di soddisfazione degli utenti.
2.8. *Sviluppi futuri.*
I siti governativi devono essere concepiti in modo da lasciare spazio a future applicazioni tecnologiche quali la loro fruibilità attraverso altri canali diversi dalla rete Internet. Le tecnologie senza cavo e la TV digitale sono solo alcuni tra i canali di comunicazione ipotizzabili per l'accesso ai servizi offerti dalle amministrazioni pubbliche.
3. *Norme transitorie.*

Le amministrazioni che alla data di entrata in vigore della presente direttiva non risultino conformi a quanto da essa disposto, possono essere ammesse nel dominio «.gov.it» a condizione che presentino al Dipartimento per l'innovazione e le tecnologie un piano tecnico ed organizzativo di adeguamento contenente sufficienti informazioni per la valutazione dello stesso.

4. *Modalità di assegnazione del dominio.*

La modalità di assegnazione dei nomi nel dominio «.gov.it» è analoga a quanto ad oggi avviene per la registrazione di nomi nel dominio «.it» o sotto la sua struttura geografica predefinita.

La procedura di registrazione prevede l'invio da parte del richiedente del nome a dominio di una lettera di assunzione di responsabilità dell'uso del dominio stesso. La lettera dovrà essere inviata al Dipartimento dell'innovazione e tecnologie. Il Dipartimento effettuerà le dovute verifiche formali e tecniche prima di effettuare la registrazione.

Ogni altra attività relativa alla gestione dei domini, come cambio di nome, cessazione, riassegnazione, cambio di *provider/mantainer*, modifica della delega ecc. dovrà essere tempestivamente comunicata con lettera al Dipartimento.

Ulteriori informazioni, dettagli e la modulistica corrispondente sono disponibili sul sito del Dipartimento per l'innovazione e le tecnologie www.innovazione.gov.it

5. *Il portale nazionale.*

Il portale nazionale «italia.gov.it» intende realizzare la sede virtuale nella quale ciascuno possa trovare con facilità la risposta più semplice e veloce possibile alle proprie esigenze di rapportarsi con la pubblica amministrazione.

Le singole amministrazioni rimangono le uniche titolari e responsabili della erogazione dei servizi e, anzi, trovano nel portale nazionale una ulteriore e più ampia valorizzazione del proprio impegno di servizio agli utenti.

Affinché gli obiettivi del portale siano conseguiti appieno, sia in fase di lancio sia nel prosieguo, è essenziale che vi sia un impegno continuo e puntuale delle singole amministrazioni nel fornire in fase iniziale e mantenere aggiornate nel tempo le informazioni di propria competenza necessarie alla alimentazione delle diverse sezioni del portale.

In particolare, le amministrazioni e gli enti dovranno impegnarsi a fornire tempestivamente tutti gli aggiornamenti alla situazione dei servizi in linea che avranno validato alla data del 15 maggio, nonché tutti gli aggiornamenti alla descrizione testuale dell'universo dei servizi erogati; inoltre dovranno contribuire per le parti di rispettiva competenza alla alimentazione delle sezioni tematiche che verranno via via attivate.

È quindi necessario che i responsabili dei singoli siti e portali, meglio specificati al successivo punto 7, siano tenuti al corretto adempimento di tali impegni.

Perché tutto ciò si realizzi al meglio, nonché allo scopo di attivare una comunicazione bidirezionale finalizzata a fornire alle amministrazioni supporto e notizie utili all'azione di sviluppo della loro presenza in rete, è in fase di costituzione a cura del Dipartimento per l'innovazione e le tecnologie una redazione centrale del portale nazionale nonché l'infrastruttura e gli standards di interazione fra tale redazione e le redazioni dei singoli siti o portali verticali, con ciò realizzando un articolato sistema redazionale virtuale in grado di assicurare una crescita più veloce, armonica ed efficace dell'offerta di servizi pubblici in rete.

6. *Adempimenti dell'amministrazione.*

Per la corretta realizzazione delle disposizioni contenute nella presente direttiva è necessario quindi che le amministrazioni pongano in essere una serie di adempimenti. Il Dipartimento per l'innovazione e le tecnologie sarà tenuto a coordinare tali adempimenti ed a fornire il necessario supporto collaborativo e tecnico alle amministrazioni che lo richiedano. Infatti il coordinamento delle iniziative, sia all'interno dell'amministrazione, sia tra le diverse amministrazioni, costituisce, senza dubbio, un fattore critico di successo del processo in atto.

È necessario, pertanto, che ciascuna amministrazione individui strutture di coordinamento esistenti o istituisca specifiche strutture o gruppi di lavoro cui affidare l'attuazione della normativa indicata.

In particolare, l'attuazione dell'iniziativa presuppone che le amministrazioni, oltre a predisporre le opportune risorse tecnologiche, avviino cambiamenti di natura strutturale e organizzativa, che includano l'individuazione e la nomina tra i dirigenti e i funzionari in organico di un responsabile in possesso di idonei requisiti professionali o di professionalità tecnica, che controlli l'esistenza continuativa dei requisiti richiesti per la permanenza nel dominio «.gov.it», e per la corretta e tempestiva alimentazione del portale nazionale. Le amministrazioni sono a tal fine tenute a razionalizzare la struttura dei siti internet esistenti e, ove occorra, a modificare i siti, per rendere omogenei gli stessi, in modo da garantirne la migliore fruibilità agli utenti.

È evidente come il raggiungimento dell'obiettivo dipenda innanzi tutto dalla capacità di progettare in ciascuna amministrazione un vero e proprio programma di interventi di natura organizzativa e tecnologica, correttamente dimensionato alle effettive esigenze operative e che individui chiaramente responsabilità unitarie sia sui contenuti che sugli aspetti tecnici.
La piena responsabilità e sensibilità da parte degli organi di vertice delle amministrazioni è indispensabile per l'attuazione delle soluzioni che incideranno anche professionalmente sul tessuto organizzativo.
A tal fine è necessario che, in sede di definizione di priorità e degli obiettivi ai sensi dell'art. 4, comma 1, lettera *b*), del *decreto legislativo 30 marzo 2001, n. 165*, e successive modifiche si proceda da parte degli organi di direzione politica ad attribuire alle sopra indicate strutture specifici obiettivi finalizzati all'attuazione della presente direttiva.
7. *Amministrazioni aventi diritto.*
La presente direttiva è indirizzata a tutte le amministrazioni centrali dello Stato ed agli enti pubblici sottoposti alla vigilanza ministeriale. La direttiva intende rivolgersi ai siti di tutte le amministrazioni statali e agli enti pubblici nazionali che offrono servizi pubblici di tipo informativo/conoscitivo e transazionale ai cittadini ed alle imprese. Per le regioni e gli enti locali territoriali costituisce contributo alle determinazioni in materia, nel rispetto della loro autonomia. Può rappresentare schema di riferimento anche per le altre amministrazioni pubbliche di cui all'art. 1, comma 2, del *decreto legislativo 30 marzo 2001, n. 165*.
Va da ultimo segnalato che l'appartenenza al dominio «.gov.it» viene contrassegnata da un logo, inserito nella pagina iniziale del sito, che rappresenta graficamente lo stemma della Repubblica italiana, connotando la natura istituzionale del sito stesso.

Nomi di dominio in internet e nomi di regioni italiane

NUMERO SCHEDA: 1135

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: NOMI DI DOMINIO

FONTE: IL FORO ITALIANO

AUTORE: Paolo Laghezza

NUMERO: 12

DATA: 01/12/2001

PAGINA: 3705-3717

NATURA ATTO: COMMENTO

L'ordinanza 23 marzo 2001 del Tribunale di Siracusa ribadisce l'orientamento secondo il quale l'uso da parte di un terzo di un domain name corrispondente ad un marchio precedentemente registrato da altra impresa determina, per quest'ultima, un danno ingiusto ed immediato consistente non solo nella confusione che l'iniziativa è idonea a provocare, ma anche nell'impedire al legittimo titolare del marchio di registrarlo, a sua volta, come domain name. Tale danno può inoltre configurarsi come violazione delle norme che presiedono alla correttezza e lealtà della concorrenza (art. 2598, nn.1 e 3 cod. civ.). Il tribunale specifica, con l'occasione, i limiti e le condizioni di applicazione della normativa dettata a tutela dei marchi in materia di domain names. Innanzitutto

precisa che il titolare non deve incorrere nei divieti sanciti dalla legge e, in particolare, dall'art. 8 r.d. 929/42.
Posto che il nome di una località può costituire oggetto di marchio soltanto ove, lungi dal rivelare particolari caratteristiche del prodotto o far riferimento alla sua origine, assuma un significato fantastico con funzione meramente individualizzante, il provvedimento respinge il ricorso ex art. 700 c.p.c. proposto dal titolare del marchio"Sicilia on line" inteso ad inibire l'utilizzo dello stesso come domain name di un sito Internet. Precisa, inoltre, che il nome, sebbene registrato come marchio di servizio, si riduce ad un mero toponimo e rimanendo, quindi, privo del carattere di originalità, incorre nella nullità sancita dall'art. 47 della legge sui marchi.

Si allega il testo.

TRIBUNALE DI SIRACUSA - Sez. Dist. Lentini - 23.03.2001 (Giud. C. Catalano)

Con ricorso depositato in data 27 dicembre 2000, la GESTEL s.r.l. adiva il Giudice di Lentini, esponendo:

-di svolgere attività di gestione di servizi informatici e telematici anche a mezzo della rete Internet;

- che i servizi offerti da essa ricorrente risultavano contrassegnati dal marchio di servizio "Sicilia on Line" e "Sicily on line", graficamente rappresentato da un campo rettangolare con ivi impressa la figura della trinacria;

- che il servizio contraddistinto dal marchio la parola consisteva in "una banca dati di informazioni e servizi telematici su rete internet e su tutte le altre reti telematiche di volta in volta utilizzate ed inoltre nei collegamenti telematici ed in tutti i mezzi e forme pubblicitarie necessarie

- che tale marchio era stato regolarmente registrato presso il Ministero dell'Industria, Commercio ed Artigianato;

- che, durante il settembre precedente, essa ricorrente aveva constatato che altra ditta, appartenente all'ing. Francesco Saluta, "operante nel medesimo settore di attività ed in particolare in Internet", utilizzava anch'essa un marchio recante la dicitura "Sicily on line"

- che detto marchio era stato altresì diffuso, a scopi pubblicitari, dalla Euro Data Engineering s.r.1.(in prosieguo semplicemente EDE), con sede in Lentini, il cui indirizzo corrispondeva a quello dell'ingegnere Saluta;

- che il marchio in questione doveva considerarsi "confondibile" a quello utilizzato da essa ricorrente, e ciò per il solo fatto di recare la dicitura "Sicily on line", elemento prevalente del marchio della Gestel. S.r.l..

Svolte le superiori premesse, e precisato che "in materia di segni distintivi il periculum in mora è in re ipsa", chiedeva che il Giudice adito (al sensi dell'art 63 R.D. n. 929/42, ovvero, in subordina ai sensi dell'art. 700 c.p,c,) dichiarasse il diritto della Gestel all'uso esclusivo del marchio "Sicily on line", dichiarasse illegittimo l'uso da parte della EDE di un marchio idoneo a determinare confusione presso gli utenti dei servizi offerti da essa ricorrente, inibisse quindi alla EDE l'ulteriore utilizzo del denunziato marchio, fissasse una congrua somma per ogni violazione e per ogni ritardo nella esecuzione dell'emanando provvedimento, condannasse la società convenuta al risarcimento dei danni cagionati per effetto dell'abusiva utilizzazione del marchio ed ordinasse (secondo le modalità ritenute più opportune) la pubblicazione del dispositivo del provvedimento inibitorio.
Ritualmente costituitasi in giudizio, la EDE deduceva:
- che già in data 6 novembre 1999, la Gestel aveva proposto un ricorso avente Identico contenuto;
- che il provvedimento di rigetto di tale ricorso, reso in data 31, gennaio 2000, era divenuto definitivo;- che l'atto introduttivo del presente giudizio differiva dal primo soltanto in relazione all'identità del soggetto convenuto in giudizio (EDE, piuttosto che Saluta Francesco);- che la domanda in questione doveva considerarsi inammissibile per carenza di nuove ragioni idonee a giustificarla;- che, in ogni caso, la Gestel non aveva "alcun titolo né alcun interesse, né legittimazione a tutelare alcun marchio o domini, e tanto meno il marchio in questione ed era (è) comunque decaduta da ogni diritto";- che non rispondente a verità ed in ogni caso non provata si rivelava la circostanza secondo la quale, nel corso

dello scorso settembre, la EDE avrebbe diffuso messaggi pubblicitari avvalendosi del marchio “Sicily on line”;- che, infine, l’assegnazione dei domini sulla rete Internet doveva reputarsi assoggettata unicamente alle “Regole di Naming” predisposte dalla Naming Authorithy Italiana. Acquisiti i documenti offerti in produzione, si procedeva all’assunzione di taluni informatori. All'udienza dell'8 febbraio 2001, il Giudice si riservava di provvedere assegnando alle parti un termine per il deposito di note difensive.
Tanto premesso in ordine allo svolgimento del processo, ragioni di carattere logico-giuridico impongono di esaminare le questioni rilevanti ai fini del thema decidendum secondo l'ordine che segue: 1) asserita inammissibilità della domanda per carenza di muovi elementi, idonei a giustificarla secondo il disposto di cui all'art. 669 septies c.p.c; 2) legittimazione attiva della Gestel; 3) disciplina applicabile alla vicenda in oggetto; 4) titolo della ipotizzata responsabilità della EDE; 5) eventuale nullità del brevetto; 6) prospettata non tutelabilità del marchio; 7) sussistenza del periculum in mora.1) In ordine al primo dei profili sopra elencati, è sufficiente osservare che l'improponibilità dell'istanza prevista dal primo comma dell'art. 669 septies c.p.c. resta di per sé esclusa (anche) dalla deduzione di nuovi mezzi di prova a sostegno della domanda.Ne consegue che il ricorso per cui si procede, in quanto sopportato dalla produzione di nuove prove documentali, deve reputarsi del tutto ammissibile, E ciò non trascurando di osservare che, tenuto conto degli elementi distintivi dell’azione (petitum, causa petendi e soggetti), trattasi, comunque, di domanda diversa da quella già proposta dalla Gestel con ricorso dei 6 novembre 1999. 2) In merito alla questione riguardante la carenza di legittimazione attiva, di titolo e di interesse, ad agire in capo all’odierna ricorrente, la EDE deduce che Sicily on line e Sicilia on line rappresentano marchi registrati ormai appartenenti in via esclusiva alla Siciliaonline s.p.a., società costituitasi durante la scorsa estate.Tale circostanza risulterebbe, in particolare, corroborata dal contenuto della pagina web prodotta in giudizio dalla EDE (non contestata sotto alcun profilo dalla ricorrente e, peraltro, riconosciuta anche da uno degli informatori escussi) nella quale si rinviene la dicitura “SiciliaOnline e SicilyOnline sono marchi registrati di proprietà esclusiva di Sicilia On Line
s.p.a.". Ragion per cui la Gestel, in quanto non più proprietaria dei marchi in parola, non potrebbe vantare alcun diritto sui medesimi, né - tanto meno - agire per la relativa tutela.
L'assunto difensivo di cui sopra non merita accoglimento. E ciò in quanto la documentazione prodotta in giudizio dall'odierna ricorrente deve reputarsi di per sé idonea a comprovare che quest'ultima risulta ancora titolare del marchio consistente in "un campo rettangolare con una sovrascrittura <<Sicily On Line. Servizi in Internet>> con affianco la figura della "trinacria" per metà posta sul rettangolo" (cfr. "dichiarazione di protezione" depositata in data 18 ottobre 1995 dal signor Marco Di Marco, nella qualità di legale rappresentante della Gestel, nonché correlato "attestato di registrazione del marchio d'impresa" rilasciato dal Ministero dell'Industria, del Commercio e dell'Artigianato).
La EDE non ha, per contro, offerto in produzione prove sufficienti a dimostrare l'asserito trasferimento della proprietà esclusiva di detto marchio in favore alla Siciliaonline s.p.a.
Né, in particolare, ai suddetti fini sembra possibile attribuire il valore di prova sufficiente al contenuto della summenzionata pagina web ovvero alle dichiarazioni rese in udienza dall'ing. Paolo De Stefani. E ciò anche in considerazione della ipotizzabile eventualità che la Gestel, quale socia della Siciliaonline s.p.a., abbia consentito a quest'ultima l'utilizzo di fatto del marchio in contestazione, senza peraltro procedere ad alcun trasferimento di titolarità.
3) Più complesse considerazioni si impongono per quanto attiene alla individuazione delle norme concretamente applicabili alla vicenda in esame, dovendosi stabilire se il conflitto di cui trattasi rinvenga la propria disciplina nelle disposizioni legislative dettate in tema del marchio e degli altri segni distintivi dell'impresa ovvero esclusivamente nelle c.d. regole di naming.
Con specifico riferimento alla qualificazione giuridica del nome di dominio, la società resistente afferma che "per le enormi differenze che sussistono tra domini, marchi ed altri segni distintivi dall'impresa, la legge marchi non è comunque applicabile al caso che ci occupa", atteso che mentre il domain name "può essere formato solo da lettere o numeri e costituisce esclusivamente un indirizzo telematico che consente di raggiungere il sito da qualsiasi parte del mondo", il marchio è invece "caratterizzato da vari tipi di segni grafici che possono formare infinite combinazioni e tutela il prodotto di un'impresa", né, oltre tutto, il domain name potrebbe essere assimilato ad una insegna, giacché quest'ultima "costituisce solo un punto di riferimento dell'impresa", né, oltre tutto, il domain name potrebbe essere assimilato ad una insegna, giacché quest'ultima "costituisce solo un punto di riferimento dell'impresa in un ambito territoriale", laddove il nome di dominio "è solo un modo per rendere... <<ricordabile>> un indirizzo telematico formato da numeri;.. cioè identifica un computer collegato alla rete da qualunque parte del mondo".
Muovendo dai superiori rilievi, la EDE conclude che, nell'ordinamento italiano (in mancanza di alcuna

specifica disciplina di legge), la materia dei nomi a dominio dovrebbe reputarsi governata soltanto dalle regole sancite dalla Naming Autorithy Italiana (articolazione dell'organismo sovranazionale denominato Internet Assigned Numbers Autorithy, ovvero IANA) - più precisamente - dal principio della priorità temporale (c.d. first come, first served), alla cui stregua il domain name va assegnato a colui che per primo ne faccia richiesta.
La tesi come sopra sintetizzata trova conforto in taluni precedenti giurisprudenziali, intesi soprattutto a valorizzare il sistema tecnico operativo riguardante il funzionamento della rete Internet (Trib. Firenze, sez. distaccata di Empoli, ord. 23 novembre 2000; Trib. Firenze, ord. 29 giugno 2000).
Nel contesto delle richiamate pronunce, si sostiene che: 1) il domain name equivale semplicemente ad un indirizzo, non assimilabile al marchio né all'insegna; 2) il nostro ordinamento non tutela la corrispondenza tra marchio e dominio, cioè non tutela il diritto di registrare un domain name corrispondente al proprio marchio e non contempla, quindi, il diritto di estromettere, chi abbia già in precedenza validamente registrato (in ossequio alle regole di naming) un identico domain name; 3) il beneficio di potersi fare raggiungere dell'utente tramite semplice digitazione dell'indirizzo telematico è un beneficio"relativo" e comunque non può considerarsi tale da rendere indefettibile e tutelabile la corrispondenza fra dominio; 4) in concreto, laddove 1'utente esperto ben sa che il domain name può non corrispondere al marchio, l'utente inesperto che intenda raggiungere il sito di una determinata impresa, potrà reperirlo partendo da uno del portali esistenti ovvero attivando la ricerca da uno del numerosissimi motori; 5) in sostanza la funzione del Domain Name System è soltanto quella di consentire a chiunque di raggiungere una pagina web e, in quanto mezzo operativo e tecnico-logico, non può porsi per esso un problema di violazione del marchio di impresa, della sua denominazione o dei suoi segni distintivi.
L'iter logico su cui si fondano i precedenti giurisprudenziali in rassegna, pur offrendo interessanti spunti di riflessione, non può essere condiviso.
a) Sul punto, occorre anzitutto rammentare che il termine "segno" di cui all'art. 1 della Legge Marchi risulta utilizzato dal legislatore con un significato talmente ampio da potervi senz'altro ricomprendere qualsiasi espressione grafica o fonetica (anche se composta esclusivamente da lettere e numeri) preordinata alla individuazione di una attività di impresa.
b) Infondata deve reputarsi, inoltre, l'idea secondo la quale il marchio (a differenza del domain name) tenderebbe unicamente a tutelare il prodotto di una impresa: e ciò per la semplice considerazione che, accanto al "marchio di prodotto", esiste altresì il c.d. " marchio di servizio" (qual è quello in argomento), caratterizzato dal fatto di non essere - di norma - supportato da alcun prodotto, trovando concreto utilizzo prevalentemente in pubblicità.
c) Va poi evidenziato che la possibilità di individuare posizioni giuridiche soggettive meritevoli di tutela sussiste pur nell'ipotesi in cui si sostenga che la denominazione del sito equivalga ad un semplice indirizzo.
Non può, difatti, ragionevolmente disconoscersi che l'avvalersi nella rete Internet di un "indirizzo" già utilizzato legittimamente da terzi per contraddistinguere la propria impresa riveste i caratteri di un comportamento idonee ad ingenerare confusione presso gli utenti,
E' in altri termini, indiscutibile che l'utilizzo come domain name di un marchio in precedenza registrato da altri viola i difatti del titolare di quel marchio perché comporta l'immediato vantaggio di ricollegare la propria attività a quella del titolare del marchio stesso, sfruttando la notorietà del segno e ricavandone un indebito vantaggio.
Basti considerare, in proposito, l'ipotesi in cui il nomnne di dominio venga pubblicato (come sovente accade) tramite inserzione sui giornali o mediante la divulgazione di depliant: in questo caso, l'utente (esperto o inesperto che sia) ben può determinarsi a digitare quell'indirizzo nella ragionevole aspettativa di raggiungere, per mezzo del medesimo, l'impresa apparentemente contraddistinta da esso.
D'altra parte, l'art. 1 del R.D. n. 929/42, dopo aver previsto che "i diritti del titolare del marchio di impresa registrato consistono nella facoltà di far uso esclusivo del marchio", precisa che il titolare del marchio può comunque utilizzare il segno "nella corrispondenza e nella pubblicità" e quindi anche nella rete Internet, all'interno di un sito o come domain name (cfr., sull'argomento, tra le numerose altre, Trib. Milano, ord. 3 giugno 1997 e, in sede di reclamo, Trib. Milano ord. 22 luglio 1997; Pretura Valdagno, ord. 27 maggio 1998; Trib. Vicenza, 6 luglio 1998; Trib Napoli 8 agosto 1997; Trib, Genova ord. 23 gennaio l997; Trib. Roma ord. 9 febbraio 2000)
Deve, pertanto, ritenersi che l'adozione del marchio come nome di dominio rientri nelle prerogative del titolare.
d) Ad una identica conclusione si perviene pur nell'ipotesi in cui (per come appare plausibile) il domain name venga assimilato all'insegna (cfr., al riguardo, Trib. Milano ord. 3 giugno 1997, ove l'affinità del

norme di dominio con l'insegna viene correttamente argomentata dal rilievo che il sito configura il luogo virtuale in cui l'imprenditore contatta il cliente fino a concludere con esso il contratto), giacché si tratterebbe comunque di insegna utilizzata con funzione di marchio.
Ed invero, benché il nostro ordinamento non contempli alcuna norma che attribuisca al titolare di un marchio registrato il diritto di utilizzare quest'ultimo anche come insegna, esistono nondimeno ipotesi nelle quali l'utilizzo nell'insegna di parole o segni registrati in precedenza da terzi come marchio deve considerarsi illecito.
Trattasi, in particolare, del caso in cui l'inclusione nell'insegna (o nella ditta) delle parole costituenti il marchio altrui sia tale da determinare confondibilità di attività e prodotti (ai sensi dell'art. 2598 n. 1 c.c.) e dell'ipotesi in cui l'insegna sia espressione dei prodotti o servizi offerti dall'impresa (ipotesi, questa, nella quale la funzione tipica dell'insegna, che è quella di individuare logisticamente l'impresa, viene superata tramite una palese invasione della sfera della pubblicità o promozione dei servizi offerti) (cfr., sugli argomenti trattati, amplius Cass. n. 7958/87)
E dunque, dovendosi ritenere che l'offerta di servizi effettuata tramite rete Internet rientri nell'ambito della suddetta sfera di "pubblicità e promozione", coerentemente al disposto di cui all'art. I n. 2 della c.d. Legge Marchi (nella parte in cui prevede che il titolare del marchio ha il diritto di vietare a terzi di utilizzare il segno nella corrispondenza commerciale e nella pubblicità"), è inevitabile formulare un giudizio di illiceità rispetto al comportamento di colui che utilizzi come proprio nome di dominio un marchio appartenente ad altro imprenditore,
4) Tanto promesso in ordine all'astratta configurabilità del contestato illecito (scaturente, per come sopra notato, dall'utilizzo del termine Sicilyonline in funzione di presentazione immediata dei servizi offerti), si configura l'ulteriore, problema di accertare se, nella fattispecie, possa ravvisarsi una qualche forma di responsabilità in capo alla EDE, quale società del cui operato si avvale il titolare del sito Sicilyonline.it al fine di entrare in rete.
In proposito, la società odierna resistente assume, a propria difesa che a) le deduzioni formulate dalla Gestel muovono tutte dal rilievo che "nel sito Sicilyonline.it appare la scritta <<powered by Euro Data Enginceering S.r.l.>>"; b) tale, dicitura indica soltanto che il dominio in contestazione entra nella rete Internet avvalendosi della EDE; c) quest'ultima, in sostanza, e assimilabile ad "un giornale che accoglie al suo interno la pubblicità fatta da varie ditte", ovvero ad "un grande contenitore che comprende al suo interno centinaia di siti, ognuno dei quali avendo bisogno di sofisticate attrezzature tecniche per entrare in Internet, si serve di quelle messegli a disposizione dietro corrispettivo, da EDE"; d) ne consegue che detta società "non può rispondere all'operato del titolare del sito Sicilyonline.it né ha alcuna possibilità di intervento sullo stesso e di disposizione dello stesso.
La trama difensiva in oggetto va esaminata sotto due differenti profili.
Anzitutto, da un punto di vista astratto, lo specifico illecito di cui si discute, tenuto conto dei caratteri che lo connotano, oltre ad essere inquadrabile nell'ambito della disposizione ex art. 1 Legge Marchi può essere ricondotto anche alla (differente) previsione dell'art, 2598 2.c.c., il quale espressamente statuisce che "ferme le disposizioni che concernono la tutela dei segni distintivi e dei diritti di brevetto, compie atti di concorrenza sleale chiunque usa nomi o segni distintivi idonei a produrre confusione con i nomi o i segni distintivi legittimamente usati da altri
Il n° 3 della citata disposizione prevede inoltre che l'illecito concorrenziale possa essere compiuto anche indirettamente, cosicché chi collabora nel compimento di tale illecito risponde in solido con l'autore diretto.
Di conseguenza, il terzo che (senza essere ausiliario o dipendente) coopera con l'imprenditore autore "diretto" dell'atto di concorrenza sleale, fornendogli i mezzi idonei (anche mediante la realizzazione di atti semplicemente preparatori o agevolativi) risponde solidalmente dell'illecito.
Tale corresponsabilità (secondo l'indirizzo giurisprudenziale da ritenere preferibile) deve essere comunque ancorata alla sussistenza dei requisiti soggettivi previsti in materia di illecito aquiliano, richiedendosi, pertanto, che il terzo abbia operato (dolosamente o colposamente) a danno di un imprenditore ed a vantaggio di un altro (cfr., in riferimento alla componente psicologica della responsabilità solidale in discorso, Cass. Sez. Un n° 2018/85 e Cass. n° 13623/91).
La concreta applicazione dei summenzionati principi di diritto induce a ritenere che la EDE, nell'avere offerta al titolare del sito Sicilyonline.it la possibilità tecnica di accedere alla rete internet, abbia per ciò stesso integrato la componente oggettiva della descritta fattispecie di corresponsabilità.
Quando al profilo psicologico della medesima, non costituisce oggetto di specifica contestazione (e risulta peraltro adeguatamente dimostrata) la circostanza che la EDE abbia "accolto" il sito in discussione nel proprio ambito, autorizzando, consentendo o - comunque - agevolando la diffusione dei messaggi pubblicitari commissionati dal titolare del sito stesso.

In proposito, per come suggerito anche dal procuratore della società resistente, deve osservarsi che la rete Internet, quale "sistema internazionale di interrelazione tra piccole e grandi reti telematiche" può essere equiparata ad un organo di stampa (cfr., Trib. Napoli, 17 marzo 1997).
E' noto inoltre che il proprietario di un canale di comunicazione destinato ad un pubblico di "lettori" (o, nel caso di Internet, utenti) ha precisi obblighi di vigilanza sul compimento di atti di concorrenza sleale eventualmente perpetrati attraverso il canale medesimo.
In particolare, il proprietario dell'organo di comunicazione è corresponsabile con l'imprenditore, autore dell'illecito concorrenziale, quante volte il contenuto della pubblicazione integri oggettivamente gli estremi della concorrenza sleale ovvero l'inserzionista non risulti legittimo titolare del segno distintivo utilizzato (cfr., su tali aspetti, Trib. Milano decr. 29 aprile e trib. Milano ord. 31 gennaio 1980): e ciò in quanto grava sull'editore un obbligo di diligente verifica circa la "legittima titolarità del segno distintivo da parte dell'inserzionista" ed un onere di "controllo preventivo in ordine al contenuto del messaggio, al fine di verificare che la pubblicità sia palese, veritiera e corretta" (cfr., pronunce testé citate e Trib. Napoli, ord. 15 giugno 1994).
Nell'ipotesi concreta, può quindi ravvisarsi, in capo alla EDE, un difetto di diligenza, consistito nell'avere trascurato di verificare la legittima titolarità del marchio Sicilyonline.it in capo al soggetto che di esso si è avvalso.
Giova rilevare, condividendo le osservazioni di attenta dottrina, che l'eccezionale diffusività del mezzo di comunicazione di cui rende di per sé ancor più penetrante il summenzionato onere di vigilanza e, pertanto, ancor più censurabile il difetto di adeguato controllo.
Prescindendo dai superiori rilievi (e pur sostenendo la giuridica impossibilità di esigere da parte di un provider gli stessi obblighi di controllo posti a carico dell'editore), nella vicenda concreta e comunque da ritenere che la EDE, sia essa stessa titolare del sito Sicilyonline.it ovvero intrattenga con il titolare di detto sito rapporti di collaborazione ben più intensi rispetto a quelli esistenti con tutti gli altri soggetti che entrano nella rete Internet avvalendosi della EDE stessa.
Più precisamente, gli acquisti elementi di giudizio consentono di affermare che la EDE, lungi dall'avere semplicemente offerto al titolare del contestato sito i "mezzi tecnici" occorrenti per entrare in rete, abbia posto in essere una complessa attività di promozione e divulgazione, tramite la quale ha rilevato espressamente il proprio stretto legame con Sicilyonline.it. Al riguardo, è sufficiente richiamare taluni brani delle stampe tratte dal portale Sicilyonline.it (stampe offerte in produzione dalla Gestel), ove - tra l'altro - si enuncia in modo esplicito "utilizzando il nostro portale Sicilyonline.it, spiega Francesco Saluta, proprietario e amministratore di Euro Data Enginnering; "Euro Data Engineering dà vita al portale Sicilyonline.it"; "Sicilyonline.it. è una iniziativa di Euro data Engineering s.r.l.";"Facendo leva sul suo portale ora Euro data Engineering si prepara ad estendere il servizio di connettività gratuita".
Il rapporto di "appartenenza" assai verosimilmente sussiste tra Sicilyonline.it e la EDE induce a considerare infondato l'assunto difensivo secondo il quale "non si può certo ritenere che la EDE s.r.l. risponda dell'operato di tutti i siti, tra cui Sicilyonline.it, che entrano nella rete attraverso i suoi strumenti".
Sulla scorta delle prove di cui innanzi, in breve, è legittimo supporre che Sicilyonline.it, a differenza di qualsiasi altro sito che accede in Internet tramite la EDE, rappresenti uno specifico strumento del quale quest'ultima si serve per il conseguimento di propri obiettivi e rispetto al quale, di conseguenza, la resistente medesima può e deve compiere ogni verifica necessaria ad impedire la violazione di altrui diritti.
5) In riferimento all'eccezione di illegittimità, nullità o decadenza del marchio, la complessa trama difensiva proposta dal procuratore della EDE può essere schematizzata nei termini che seguono: a) il brevetto del marchio "Sicily On Line, Servizi in Internet" è stato illegittimamente concesso, giacché trattasi di marchio sprovvisto dei caratteri di originalità e novità richiesti dalla Legge Marchi; b) a tale conclusione si perviene sia muovendo da una analisi avente ad oggetto separatamente le singole parole utilizzate (Sicily On Line, servizi in Internet), sia considerando l'espressione in argomento nella sua interezza; c) dal primo punto di vista, è agevole rilevare che: la parola Sicily si limita a segnalare la provenienza geografica dei servizi offerti; la locuzione on line serve soltanto ad indicare (con terminologia ormai invalsa nell'uso comune) il collegamento alla rete Internet, la frase servizi in Internet riveste, infine, valore meramente descrittivo; d) la dedotta carenza di originalità vale anche in riferimento all'intera espressione Sicily On Line, Servizi in Internet complessivamente esaminata, atteso che nemmeno l'unione di dette parole può considerarsi tale da imprimere all'insieme di esse qualità differenti dalla semplice, e generica descrizione dell'attività posta in essere; e) né, d'altra parte, sembra, sembra possibile attribuire carattere distintivo alla figura della trinacria, in sé idonea soltanto a rappresentare la Sicilia mediante una immagine ormai da tempo appartenente alla cultura di tale

isola; f) il brevetto concesso alla Gestel va, ritenuto nullo ai sensi dell'art. 47 L.M. ovvero decaduto a mente dell'art. 41 della legge medesima, o deve - comunque - considerarsi "volgarizzato".
Le suddetti argomentazioni attengono, per com'è evidente, al fumus boni iuris dell'azionata pretesa, implicando esse la necessità di accertare (tramite la delibazione sommaria che è propria del giudizio cautelare) l'insussistenza dell'altrui "apparente" diritto a cagione delle invocate cause di nullità o decadenza del marchio.
Con specifico riferimento alla dedotta nullità, trattasi di verificare se al marchio oggetto della chiesta tutela possa ascriversi un difetto di "novità", ovvero un carattere non distintivo o meramente descrittivo (cfr. artt.17, 18 e 47 L.M.).
In proposito, reputa il decidente che i rilievi formulati dalla EDE meritino accoglimento, dovendosi ritenere che la frase costituente il marchio in discussione (valutata nella sua globalità) non sia idonea a racchiudere e comunicare messaggi nemmeno in parte diversi dalla mera, ed oltre modo generica, descrizione del servizio offerto e della località geografica di relativa provenienza.
Riguardo alle ragioni di tale convincimento, deve preliminarmente evidenziarsi - da un lato - che l'espressione on line, ad esito del celere processo di volgarizzazione che ne ha determinato la definitiva acquisizione al linguaggio comune, si limita a denotare (in forza di una semplice sinonimia) il collegamento alla rete Internet, e - dall'altro - che nulla aggiunge al suddetto significato la precisazione "Servizi in Internet", deputata a designare soltanto l'offerta di servizi tramite il summenzionato canale di comunicazione (come già potrebbe evincersi dai termini on line).
Ragion per cui l'indagine in parola va incentrata sul termine Sicily (o Sicilia) (alla medesima stregua di quella indagine che, esemplificativamente riferita a prodotti da forno denominati "Biscotti Baby", dovrebbe attenere essenzialmente alla parola "Baby").
Ciò premesso, in ordine all'utilizzo di nomi geografici, l'art. 18 L.M. espressamente statuisce che " non possono costituire oggetto di registrazione come marchio di impresa ... i segni costituiti esclusivamente dalle denominazioni generiche di prodotti o servizi o da indicazioni descrittive che ad essi si riferiscono, come i segni che commercio possono servire a designare la provenienza geografica ... del prodotto o della prestazione del servizio…".
La portata del precetto in argomento, sulla scorta di principi giurisprudenziali ormai consolidati, va intesa nei termini che seguono: a) il marchio, per definizione, vale ad identificare uno specifico prodotto o servizio come proveniente da uno specifico produttore, a prescindere dalla relativa origine geografica; b) l'art. 18 L.M. annovera, tra le possibili indicazioni descrittive vietate dalla legge, anche le denominazioni geografiche; c) l'utilizzo in funzione descrittiva della denominazione geografica ricorre ove quest'ultima si limiti ad indicare il luogo geografico in cui il servizio o il prodotto è realizzato; d) la denominazione di una località geografica può, pertanto, costituire marchio brevettabile ogni qualvolta essa, lungi dall'esprimere un semplice riferimento all'origine logistica del prodotto o servizio, venga adoperata in modo simbolico o metaforico, ovvero si risolva in un accostamento di pura fantasia atto a conferire carattere originale di efficacia individuazione (cfr., tra le numerosissime altre Cass. n° 5462/82; 591/92; 11017/92; 9882/93; 10587/96).
I suesposti canoni di giudizio autorizzano a sostenere che il marchio di cui si discute, in quanto toponimo rimasto tale (ossia non adoperato in senso rappresentativo di qualità, caratteri o pregi del servizio contrassegnato), impinga nella sanzione di nullità comminata dall'art. 47 L.M.
Né, ad escludere tale conclusione, è possibile richiamare la componente figurativa del marchio stesso (costituita dall'emblema della trinacria), giacché trattasi di simbolo appartenente al patrimonio culturale dell'intera collettività, notoriamente destinato ad evocare la Sicilia ed utilizzato quale vero e proprio emblema ufficiale di detta Regione.
Il profilo da ultimo esaminato suscita peraltro la necessità di approfondire la tematica inerente ai rapporti tra la normativa sui marchi e la tutela di cui gli stessi possono fruire allorché si verta in tema di segni distintivi preordinati ad assolvere esclusivamente la funzione di indirizzo telematico.
Al riguardo, in attesa di una compiuta normativa di raccordo tra le disposizioni dettate dalla Legge Marchi e la disciplina consacrata dalle regole di naming, è plausibile ritenere che, nel caso di marchi unicamente intesi ad un utilizzo come nomi di dominio, l'apprezzamento relativo ai requisiti legittimanti alla registrazione (di cui alla Legge Marchi) debba svolgersi ponendo in secondo piano l'esame inerente alla struttura grafico - ornamentale. E' ciò in quanto: a) il nome di dominio può essere composto soltanto da cifre e/o lettere, e non anche da immagini; b) tale circostanza fa si che il pubblico di utenti della rete Internet (destinatario dei messaggi promozionali relativi ai domain names) tenda a memorizzare in via esclusiva l'insieme dei simboli da digitare sulla tastiera del computer al fine di accedere al propagandato sito: l'approccio psicologico degli utenti Internet appare, in altri termini, del tutto disancorato dal fascino suggestivo che la particolare grafica utilizzata sembrerebbe in grado di

esercitare; c) già dal punto di vista generale ed astratto, allora, intercorre una sensibile diversità tra marchi destinati a contraddistinguere un prodotto (e, quindi, ad esercitare sul pubblico dei consumatori quella particolare forza attrattiva che scaturisce dalla forma, dai colori e dal pregio ornamentale esterno della confezione o dell'imballaggio) e marchi distintivi di un servizio offerto tramite rete Internet; c) ne deriva che un problema di confondibilità tra segni può prospettarsi soltanto allorquando si tratti di sequenze numerico-letterali assai simili, indipendentemente dalle rappresentazioni figurative adoperate in sede di propaganda (tanto più se si tiene conto della circostanza che, quasi sempre, la concreta diffusione di un nome di dominio viene attuata tramite la mera indicazione della relativa sequenza, nel contesto di articoli di giornale ovvero nell'ambito di programmi radiotelevisivi); d) dai superiori rilievi sembra, in conclusione, potersi argomentare il principio secondo il quale la normativa contenuta nel R.D. n° 929/42 (ancorché tuttora applicabile), ogni qualvolta si controverta su marchi utilizzati soltanto come nomi di dominio, debba comunque subire una sorta di "adattamento" alla realtà presa in considerazione, adattamento consistente nel negare all'elemento figurativo quella stessa rilevanza che il medesimo riveste in tutti gli altri settori del commercio.
Diversamente opinando, nessuna tutela sarebbe possibile accordare al titolare di un "marchio - nome di dominio" a fronte dell'utilizzo di altro domain name assai diverso per quanto attiene alle immagini di contorno, ma notevolmente simili con riguardo a quella parte di esso che occorre digitare sulla tastiera del computer per accedere al virtuale luogo di acquisto di beni o servizi.
Giova infine soggiungere, ad ulteriore conforto della sopra formulata valutazione di nullità del marchio appartenente alla Gestel, che, nell'ipotesi in argomento, non sussistono nemmeno elementi di giudizio sufficienti a far considerare, integrati gli estremi dell'uso riabilitante di cui all'art. 47 bis L.M. (norma che recepisce il fenomeno del c.d. secondary meaning, di origine anglosassone, implicante la valorizzazione come marchio di un termine originariamente comune, in virtù dell'intenso uso fattone e, quindi, della notorietà di cui gode presso il pubblico).
Sotto tale profilo, alla luce del quadro probatorio emerso dall'espletata istruttoria, può anzi rilevarsi come soltanto la EDE (e non anche la ricorrente) abbia curato una intensa propaganda del contestato marchio.
Le considerazioni di cui innanzi, in quanto sufficienti a far escludere la probabile fondatezza della pretesa fatta valere dalla Gestel, rendono superfluo l'esame delle ulteriori questioni sollevate da controparte.
Ragioni di completezza espositiva suggeriscono, ciò non di meno, di estendere anche ad esse la presente indagine.
Relativamente all'ulteriore eccezione di non tutelabilità del marchio, la società odierna convenuta ha osservato che: 1) il marchio registrato dalla Gestel, se anche legittimamente concesso, non potrebbe in ogni caso reputarsi tutelabile, in quanto trattasi di marchio tuttora "debole", rispetto al quale l'usurpazione o la contraffazione (e quindi la confondibilità) debbono ritenersi escluse anche in presenza di lievi modificazioni o aggiunte; 2) nella fattispecie che ci occupa i due segni in conflitto presentano una differente veste grafica ed implicano l'utilizzo di parole diverse (l'uno Sicily On Line, Servizi in Internet e l'altro Sicilyonline.it); 3) non v'è, pertanto, spazio per la chiesta tutela, la quale può concedersi esclusivamente nei riguardi di una imitazione del tutto servile.
Le argomentazioni di cui innanzi debbono reputarsi infondate.
Non sembra, anzitutto, oggettivamente contestabile (per come risulta già evincibile dai rilievi svolti circa l'esaminata eccezione di nullità) il fatto che la locuzione caratterizzante il marchio della Gestel presenti una diretta aderenza concettuale con i servizi cui inerisce e con la relativa regione di provenienza.
La modesta originalità del summenzionato marchio consente di riconoscere al medesimo l'attributo di "debole" (in contrapposizione ai marchi c.d. "forti", qualificati da un notevole apporto di fantasia e, pertanto, privi di qualsiasi contenuto evocativo o significativo del prodotto o del servizio offerto).
Ciò posto, costituisce ormai ius receptum il principio secondo il quale, laddove la tutela dei marchi "forti" deve riferirsi al loro "nucleo ideologico", i marchi "deboli", per contro, proprio perché dotati di minore originalità, risultano tutelabili soltanto se riprodotti integralmente ovvero imitati in modo molto prossimo.
Ne consegue che, ove si verta in materia di segni deboli, l'accertamento della contraffazione va condotto secondo criteri di minor rigore, di talché anche minime modiche di contorno possono reputarsi sufficienti a far escludere l'integrale imitazione.
Occorre, per altro verso, rammentare che il giudizio di confusione tra i marchi (ancorché deboli) va comunque collegato alla generale "impressione" che i medesimi sono in grado di suscitare presso i consumatori del prodotto o gli utenti del servizio rappresentano dai segni, tenendo conto delle qualità,

dei valori o delle caratteristiche comunicate da essi e delle associazioni mentali o suggestioni evocate: ragion per cui l'apprezzamento in discorso va rivolto alle connotazioni salienti dei marchi, quali emergono da una valutazione sintetica ed unitaria dei singoli elementi costitutivi, avuto riguardo altresì al tipo ed al livello medio di percezione dei soggetti ai quali il prodotto o il servizio è destinato.
Sulla scorta degli enunciati criteri di giudizio, è gioco forza sostenere che il marchio Sicilyonline.it rappresenti una imitazione pressoché servile del marchio Sicily on line, Servizi in internet. Ed invero, quanto al profilo terminologico, la dissomiglianza tra i marchi in oggetto non appare riconducibile al mero fatto che la EDE abbia omesso, dal corpo del marchio da essa adoperato, la locuzione "Servizi in Internet".
Una siffatta modifica non riveste, difatti, portata idonea a differenziare neanche marginalmente i due marchi, atteso che (per come sopra diffusamente notato) la predetta frase si rivela come una sorta di parziale sinonimo dei termini on line, indicativi del collegamento in rete a mezzo del quale è operata l'offerta di servizi.
E' appena il caso di osservare poi che nessuna attitudine distintiva è possibile poi riconoscere alla particella .it (intesa ad indicare il c.d. top level domain name), attenendo essa unicamente alla locazione geografica dell'elaboratore (cfr., in tal senso, Trib. Milano ord. 3 giugno 1997).
Quando ai rispettivi elementi grafici dei due marchi sottoposti a raffronto, soccorrono invece le identiche riflessioni già riportate in tema di connotazioni distintive dei marchi aventi esclusiva funzione di domain names, riflessioni idonee a giustificare l'irrilevanza (o la scarsa rilevanza) della diversa veste figurativa dei segni.
7) Và, infine , esaminato il profilo attinente al periculum in mora.
Per com'è noto, in materia brevettuale, suole affermarsi che il requisito del periculum si rivela insito nel fenomeno contraffattivo, di per sé idoneo a determinare effetti pregiudizievoli sui rapporti di mercato. Tale enunciato, in linea di principio corretto, si rivela tuttavia suscettibile di smentita ogni qualvolta (come nella fattispecie per cui si procede) il ricorrente abbia mantenuto per un considerevole periodo di tempo un atteggiamento di sostanziale tolleranza rispetto alla violazione costituente poi oggetto di censura.
Ed invero, se l'urgenza del provvedere si concreta nella necessità di evitare quelli effetti pregiudizievoli che si produrrebbero in modo irreversibile durante il tempo occorrente alla definizione del giudizio, è lecito dubitare circa la ricorrenza di una siffatta necessità quante volte il soggetto assertivamente leso dalla contraffazione abbia manifestato un totale disinteresse rispetto a quest'ultima, così lasciando vanamente trascorrere lo spatium temporis potenzialmente idoneo a consentire l'emanazione della definitiva pronuncia di merito.
Tenuto conto di tale premessa, rilievo sintomatico deve attribuirsi alla circostanza che la Gestel, benché consapevole dell'illecito concorrenziale in parola già il 6 novembre 1999 (data alla quale risale il deposito del ricorso erroneamente proposto nei confronti di un soggetto diverso dalla EDE), abbia atteso oltre un anno per azionare nuovamente il diritto all'uso esclusivo del proprio marchio.Sembra, pertanto, potersi affermare che, nella fattispecie, la corrente equiparazione "periculum-contraffazione" abbia smarrito la propria ragion d'essere, proprio a cagione della duratura inerzia serbata dalla ricorrente (la quale, nella sua complessità, se opportunamente eccepita, ed in concorso con i necessari elementi dimostrativi, avrebbe potuto altresì inquadrarsi entro l'ipotesi di decadenza specificamente prevista dall'art. 42, n° 1, L.M.).8) Il rilevato difetto di fumus boni iuris (per presumibile nullità del marchio registrato dalla Gestel) e la ritenuta carenza di periculum in mora legittimano il rigetto del ricorso.Quanto alle spese di lite, reputa il decidente che sussistano giusti motivi per compensarne l'intero importo tra le parti in causa.

P.Q.M.

Rigetta il ricorso, compensando interamente tra le parti le spese processuali.

Ordinanza del tribunale civile di Firenze del 29 giugno 2000 sui nomi a dominio

NUMERO SCHEDA: 783

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: NOMI DI DOMINIO

FONTE: INTERLEX

NATURA ATTO: ORDINANZA

DATA ATTO: 29/06/2000

ORGANO: TRIBUNALE

L'ordinanza registra un'inversione di tendenza nell'orientamento giurisprudenziale precedente che era uniforme nello stabilire l'applicabilità delle leggi sui marchi ai casi di domain grabbing. Secondo il Tribunale di Firenze la corrispondenza marchi-dominio non è un bene assoluto e , soprattutto, non è un principio positivamente sancito nel nostro ordinamento. E, quindi ritiene che la funzione del Domain name System sia quella di consentire a chiunque di raggiungere una pagina web e, in quanto mezzo operativo e tecnico logico non può porsi per esso un problema di violazione del marchio d'impresa, della sua denominazione o dei suoi segni distintivi.

Si allega il testo dell'ordinanza.

Tribunale di Firenze –
Ordinanza del 29 giugno 2000

La N.V. Sabena S.A., con sede in Belgio in av. E. Mounierlaan, Brussels, ha chiesto provvedimento cautelare ex artt. 700 c.p.c., 63 R.D. 21/06/42, n. 929.
Sosteneva di essere titolare di marchio internazionale "Sabena", registrato l'08/10/93, valido anche in Italia e di avere, tra la fine del 1999 e l'inizio dell'anno successivo, deciso di pubblicizzare e commercializzare i propri servizi in Italia anche attraverso un sito internet, realizzato appositamente per l'utenza italiana.
Fra le regole adottare dalla Naming Aythority italiana figura il principio first come, first served, per effetto del quale un determinato domain name può essere registrato a nome di un unico soggetto, che ne diventa detentore esclusivo, e viene assegnato in base alla priorità cronologica della richiesta. Principio derivante in modo necessario dallo stesso protocollo di comunicazione utilizzato da internet, basato su una sequenza numerica univoca (IP number) tale da rendere possibile l'identificazione e l'accesso del computer cui sia assegnato un determinato IP number alla generalità di tutti gli altri computer connessi in rete. Per agevolare l'utilizzo della rete, la navigazione, all'IP number è stato affiancato un altro sistema, il DSN (Domain name System), basato sulle lettere dell'alfabeto con le quali possono essere composte parole anche di senso compiuto, quali nomi, denominazioni identificative di organizzazioni, imprese, ecc.,
In applicazione del principio first come, first served, la Registration Authority italiana rigettava la domanda di registrazione del nome formulata dalla ricorrente per attivare il proprio sito internet, in quanto il nome a dominio www.sabena.it risultava già essere stato assegnato in data 26/01/2000, alla agenzia A&A di Castellani Alessio.
Chiedeva quindi che venisse vietato alla predetta l'uso in qualsiasi forma, anche sulla rete internet, del marchio "Sabena", vietando l'utilizzazione del nome di dominio internet www.sabena.it; che le venisse ordinato di rinuciare all'assegnazione del domain name www.sabena.it, con fissazione di una penale per ogni giorno di ritardo nell'esecuzione del provvedimento; in subordine, o nel caso di mancata spontanea ottemperanza, ordinare alla Registration Authority italiana di revocare l'assegnazione del domain name www.sabena.it alla Agenzia A&A di Castellani Alessio e registrarlo a nome dela ricorrente. Inaudita altera parte veniva emesso decreto con cui si inibiva a Castellani Alessio l'utilizzo del nome di dominio da lui registrato www.sabena.it
Venivano ritualmente convocate le parti e l'Agenzia A&A di Castellani Alessio si costituiva contestando in diritto quanto dedotto dall'avversaria. Veniva quindi concesso ulteriore termine per il deposito in cancelleria di memorie e repliche.

Punto nevralgico della decisione, nella presente sede cautelare, è lo stabilire se esista nell'ordinamento italiano il diritto di registrare un domain name corrispondente al proprio marchio, così tutelandolo, pretermettendo ed estromettendo chi abbia già validamente registrato quello stesso domain name in precedenza.
Le norme di internet costituiscono un ordinamento fondato su regole di contenuto strettamente tecnico. Fra queste il ricorrente stesso ha ricordato la regola dell'unicità del dominio ed il principio, adottato dalle Autorità che provvedono alla registrazione dei nomi a dominio, del first come, first served. Non vi è dubbio che, in quanto genericamente attività umana, anche la produzione e presentazione di pagine o siti sul web non sfugga a regole dell'ordinamento giuridico generale, relative per es. all'ordine pubblico o al buon costume, salve, naturalmente, le enormi difficoltà di attuazione ed esecuzione di qualunque tutela, data la caratteristica costitutiva di internazionalità della rete. Siti inneggianti al nazzismo, per esempio, ben potrebbero essere considerati contrari all'ordine pubblico e conseguentemente sanzionati. Ma, come si vede, ne deriverebbe esclusivamente una questione di contenuti di un determinato sito web.
Cosa diversa, invece, è considerare lo stesso domain name, traduzione in qualche modo testuale dell'IP number, come parte di una sfera individuale tutelabile ovvero sanzionabile e, in ogni caso, giuridicamente rilevante.
Giurisprudenza e dottrina largamente maggioritarie hanno ritenuto in effetti che tale debba essere considerata la registrazione di un dominio, ritenendo conseguentemente applicabile la legge sui marchi, anche in sede di cautela. La dottrina, tuttavia, ha di gran lunga prevalentemente esaminato la questione partendo dalle posizioni della tutela del marchio nel diritto industriale, dalle posizioni di impresa. La domanda che più frequentemente risulta dai contributi presenti sullo steso web è: come può essere tutelato il marchio anche su internet? E si è data una risposta nel senso che sia possibile considerare il domain name parte integrante fra gli elementi individuativi della persona, parte del patrimonio personalitario.
Occorre invece, a questo punto, domandarsi se sia forse qualcosa di più che insolito, strano, curioso o bizzarro che Registration Authority e Naming Authority, gli organismi che consentono a internet di esistere e svilupparsi, considerino invece il domain name alla stregua di un mero indirizzo, un mero numero di telefono, sia pure tradotto in lettere alfabetiche.
L'elemento funzionale, operativo, non sembra affatto poter essere semplicemente obliterato. Il domain name è l'indirizzo internet di un computer collegato alla rete. Le pagine del sito internet prodotte dal soggetto che utilizza quel computer esporranno al pubblico l'attività di quel soggetto, offriranno i suoi servizi on line, esibiranno la sua denominazione.
Mediante il domain name solamente si raggiungerà quel sito, non diversamente, si potrebbe opinare, da quanto avviene raggiungendo un certo numero civico di una certa via per andare a trovare qualcuno o comporre un numero di telefono per parlare con una data persona. Il beneficio di potersi far raggiungere dall'utente-cliente digitando direttamente un nome sulla form del browser è relativo e opinabile e non tale da rendere comunque indefettibile e tutelabile la corrispondenza fra marchio e dominio. L'utente esperto, infatti, sa perfettamente della possibile non corrispondenza, in un'infinità di casi, fra dominio e marchio o denominazione d'impresa esposti e corrispondenti al sito cui vuole collegarsi. L'utente inesperto, che voglia comunque raggiungere il sito di un'impresa determinata, per esempio per fruire dei suoi servizi on line, potrà altrettanto se non più agevolmente reperirlo partendo da uno degli innumerevoli portali oggi esistenti ovvero, come impone la normale consultazione del web da quando questo esiste, attivando la ricerca da uno dei numerosissimi motori. Ciò in quanto la visibilità e reperibilità di un determinato sito internet è data essenzialmente dal suo contenuto, fra cui anche il marchio e/o la denominazione d'impresa, non meno che dal domain name.
E che corrispondenza fra marchio o denominazione di impresa non vi sia in una infinità di casi è facilmente verificabile, appunto, con una semplice ricerca su un apposito motore, come, per quanto attiene ad esempio al comparto bancario, risulta manifesto per i siti del Banco Ambrosiano Veneto (www.ambro.it), del Credito Italiano (www.credit.it), dell'Istituto di Credito San Paolo di Torino (www.sanpaolo.it) e della Banca di Roma (www.bancaroma.it), così come si può constatare dalle stampe che seguono.
In sostanza, la corrispondenza marchio-dominio, non è un bene assoluto, non è un valore assoluto e, soprattutto, non è un principio positivamente sancito nel nostro ordinamento, tanto che moltissime imprese, consce delle possibilità che la rete offre ben al di là della corrispondenza di cui si discute, puntano su altro, cioè sulla qualificazione e apprezzamento del proprio sito, sui servizi offerti on line, sui collegamenti ad altri siti e/o servizi comunque utili per l'utenza. Tanto che, proprio per regolare il settore, sono stati recentemente predisposti dei disegni di legge già presentati al Parlamento. Ma finché

internet in Italia non è regolata, normata ed in qualche modo inclusa nell'ordinamento giuridico generale, questo Giudice è convinto che gli aspetti operativi, tecnici e logici propri del Domain name System prevalgano sull'utilità che la singola impresa può ricavare dalla corrispondenza nome-dominio; che tali aspetti operativi, tecnici e logici assimilino più il domain name ad un indirizzo che ad un segno identificativo di un soggetto. Questo Giudice è convinto, in sostanza, che la funzione del Domain name System sia quella di consentire a chiunque di raggiungere una pagina web e, in quanto mezzo operativo e tecnico-logico, non può porsi per esso un problema di violazione del marchio di impresa, della sua denominazione o dei segni distintivi.
È d'altra parte la natura interattiva di internet, la cui effettiva dimensione non sembra essere stata ancora valutata a pieno, che desta perplessità in relazione ai precedenti giurisprudenziali. Non si digita un nome sulla form del browser di navigazione per arrivare ad ogni sito desiderato come si cambia canale TV premendo un tasto, né si può pretendere che la rete sia o che diventi così, date le sue proprie caratteristiche di unicità del dominio ed il conseguente principio first come, first served per la registrazione del domain name, che non è qui in discussione. Soprattutto il processo di reperimento del sito non si può pretendere che sia sempre e necessariamente diretto dall'esterno rispetto all'utente, cioè dalle imprese che riuscissero, in ipotesi, tutte quante a registrare il dominio corrispondente al proprio marchio. Il fumus non sussiste, il ricorso dovrà essere rigettato, l'inibitoria concessa revocata ed il ricorrente condannato alle spese del presente giudizio che si liquidano in dispositivo.

P.Q.M.

visti gli artt. 669 septies, c.p.c

RIGETTA

il ricorso e per l'effetto revoca il proprio precedente decreto in data 12-13/04/00.
Pone le spese del presente procedimento, che liquida in complessive £ 1.200.000, di cui £ 100.000 per spese

Firenze, lì 29/06/00.
Il Giudice
(Roberto Monteverde)

CAPITOLO II

PROCESSO TELEMATICO

Per processo telematico si intende la possibilità che, nell'ambito del processo civile, viene data alle parti, al giudice e alla cancelleria, di formare, comunicare e notificare gli atti processuali con mezzi informatici.

La normativa principale in materia è costituita dal d.p.r. D.P.R. 13 febbraio 2001, n. 123, "Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti".

L'articolo 2 del Regolamento citato stabilisce, al primo comma, che "è ammessa la formazione, la comunicazione e la notificazione degli atti del processo civile mediante documenti informatici nei modi previsti dal presente regolamento".

Il secondo comma chiarisce che, fatto salvo quanto previsto dall'articolo 6, "l'attività di trasmissione, comunicazione o notificazione dei documenti informatici è effettuata per via telematica attraverso il sistema informativo civile".

L'art. 19 stabilisce che le disposizioni del regolamento si applicano ai giudizi iscritti a ruolo dopo il primo gennaio 2002.

Il tanto atteso decreto del ministero della Giustizia 14 ottobre 2004, ha infine dettato le "Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile".

Ampio spazio al progetto concernente il processo telematico viene dato nel piano triennale per l'informatica per gli anni 2004-2006 del ministero della Giustizia che si riporta.

" Processo telematico.

Il progetto consiste nella realizzazione di un insieme di applicazioni informatiche e infrastrutture tecnologiche che renda accessibile via web il sistema informatico civile, sia per il deposito di atti che per attività di consultazione dello stato delle cause e del fascicolo elettronico; inoltre è prevista anche la trasmissione per via telematica di comunicazioni, notifiche e copie di atti dagli uffici giudiziari ai soggetti coinvolti. La realizzazione del progetto si prefigge di:

- *consentire la consultazione a distanza dei registri di cancelleria e dei documenti contenuti nel fascicolo elettronico;*
- *consentire la richiesta a distanza di copie di documenti;*
- *consentire la trasmissione telematica di documenti da parte degli avvocati e degli ausiliari del giudice e la loro acquisizione automatica nel registro e nel fascicolo;*
- *consentire l'invio telematico degli avvisi relativi agli atti processuali compiuti;*
- *consentire la registrazione e la trascrizione telematica degli atti giudiziari;*
- *ridurre i tempi del processo attraverso il governo di questo e dell'ufficio in genere;*
- *ridurre i tempi di "attraversamento", intendendo con ciò i tempi necessari per il trasferimento degli atti sia da un ufficio all'altro sia tra uffici e soggetti esterni, inoltre l'introduzione del fascicolo elettronico riduce i tempi anche all'interno dello stesso ufficio;*
- *la razionalizzazione dei compiti degli attori del processo. Principali benefici:*
- *miglioramento della gestione del processo civile mediante l'eliminazione dei tempi di "attraversamento", con conseguente diminuzione della durata del processo fino a 6 mesi;*
- *accelerazione delle cause di almeno il 20%;*
- *recupero 30-40% di efficienza nei servizi di cancelleria;*
- *riqualificazione e razionalizzazione dell'utilizzo del personale, come conseguenza indiretta della diminuzione della attività di sportello e di mera iscrizione dati nei registri;*
- *razionalizzazione e accelerazione dei tempi di notifica, con una riduzione media di 10 giorni per notifica;*
- *miglioramento della reperibilità e fruibilità di tutti gli eventi relativi ad una causa e degli atti ad essa associati, con indiretti benefici sui tempi del processo stimabili in circa 5 mesi;*

- *semplificazione nella organizzazione degli archivi e risparmio dei costi di conservazione del materiale cartaceo;*
- *diffusione della conoscenza della giurisprudenza di merito e possibilità di confrontare le decisioni in ordine alla liquidazione dei danni, con conseguente diminuzione o eliminazione delle cause "esplorative";*
- *aumento della cooperazione tra uffici giudiziari e attori esterni.*

Volendo fare una suddivisione dei benefici per tipologia di utente:

Uffici Giudiziari

- *facilità di conoscenza dei dati e migliore governabilità degli uffici;*
- *riduzione dei tempi per l'immissione dei dati nel sistema informatico civile al fine della successiva gestione automatizzata (in quanto gli atti provenienti dall'esterno pervengono con una struttura tale da facilitarne l'elaborazione automatica);*
- *semplificazione dei controlli sui dati grazie all'ausilio di strumenti informatici;*
- *riduzione del tempo dedicato dal personale alle attività di assistenza per la consultazione e alla produzione di copie, il che fa in modo che possa dedicarsi ad altri compiti;*
- *riduzione dei tempi di comunicazione e di notifica;*
- *miglioramento dell'integrazione con gli UNEP.*

Avvocati e utenti della giustizia civile

- *estensione dell'orario di funzionamento della cancelleria (da 4h a 14h);*
- *riduzione dei tempi per la consegna di atti, che potrà avvenire in pochi minuti;*
- *consultazione on line del fascicolo elettronico e dello stato della causa, quindi maggiore rapidità e trasparenza rispetto alla situazione attuale;*

- *riduzione dei tempi per ottenere copie autentiche e non (da 3/6 giorni a 1/3 giorni).*

Esecuzioni mobiliari e immobiliari.

Il progetto ha lo scopo di realizzare un software per la completa automazione dell'attività di cancelleria e del giudice delle Esecuzioni Mobiliari e Immobiliari (gestione procedimento, gestione udienze, gestione perizie, gestione pubblicità, gestione post-aggiudicazione, gestione fasi collaterali, gestione notai delegati). L'applicativo è stato definitivamente collaudato nel dicembre 2002. Si prevede la distribuzione sul territorio entro la fine dell'anno 2005. Le linee di evoluzione del sistema sono descritte nell'ambito del progetto "Portale di accesso agli Uffici Giudiziari".

Pubblicato il decreto che detta le regole tecniche per l'uso di strumenti informatici e telematici nel processo civile

NUMERO SCHEDA: 6339

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: PROCESSO TELEMATICO

FONTE: GAZZETTA UFFICIALE

NUMERO: S.O. n. 272

DATA: 10/11/2004

RIFERIMENTO NORMATIVO: d.p.r. 123/2001

NATURA ATTO: DECRETO MINISTERIALE

DATA ATTO: 14/10/2004

ORGANO: MINISTERI

SCHEDE COLLEGATE: 703

Sul Supplemento Ordinario n. 167 alla Gazzetta Ufficiale n. 272 del 19 novembre 2004 è stato pubblicato il decreto del Ministero della Giustizia 14 ottobre 2004, che contiene "Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile", costituito da 62 articoli e due allegati.
Si segnalano, in particolare, gli articoli dedicati alla certificazione dei difensori e all'accesso dei soggetti privati abilitati, alla gestione della posta elettronica ed al ruolo dei Consigli degli ordini degli avvocati.

Si allega il testo.

L'allegato A (Regole Tecnico-Operative per l'Uso di Strumenti Informatici e Telematici nel Processo Civile) e l'allegato B (Posta certificata del processo telematico) sono consultabili al seguente indirizzo:
http://www.ilprocessotelematico.it/Indice%20Generale.htm

D.M. 14 ottobre 2004
Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile.

Capo I - Principi generali
1. Àmbito di applicazione
1. Il presente decreto stabilisce le regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile di cui all'art. 3, comma 3, del *decreto del Presidente della Repubblica 13 febbraio 2001, n. 123*.
2. Definizioni.
1. Ai fini del presente decreto si intendono per:
a) SICI: sistema informatico civile come definito nel *decreto del Presidente della Repubblica 13 febbraio 2001, n. 123*;

b) gestore centrale: struttura tecnico-organizzativa che, nell'àmbito del dominio giustizia, come definito all'art. 1, comma 1, lettera *e*) del *D.P.R. 13 febbraio 2001, n. 123*, fornisce i servizi di accesso al SICI ed i servizi di trasmissione telematica dei documenti informatici processuali fra il SICI ed i soggetti abilitati, secondo le norme riportate nel presente decreto;
c) gestore locale: sistema informatico che fornisce i servizi di accesso al singolo ufficio giudiziario o all'ufficio notifiche esecuzioni e protesti (UNEP), ed i servizi di trasmissione telematica dei documenti informatici processuali fra il gestore centrale ed il singolo ufficio giudiziario o UNEP;
d) certificazione del difensore: attestazione al difensore di iscrizione all'albo, all'albo speciale, al registro dei praticanti abilitati ovvero di possesso della qualifica che legittima l'esercizio della difesa e l'assenza di cause ostative allo svolgimento dell'attività difensiva;
e) punto di accesso: struttura tecnico-organizzativa che fornisce ai soggetti abilitati, esterni al SICI, i servizi di connessione al gestore centrale e di trasmissione telematica dei documenti informatici relativi al processo, nonché la casella di posta elettronica certificata, secondo le regole tecnico-operative riportate nel presente decreto;
f) autenticazione: operazione di identificazione in rete del titolare della carta nazionale dei servizi o di altro dispositivo crittografico, contenente un certificato di autenticazione, secondo la previsione dell'art. 62;
g) firma digitale: firma elettronica avanzata, basata su un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura, di cui al *decreto legislativo 23 gennaio 2002, n. 10*;
h) fascicolo informatico: versione informatica del fascicolo d'ufficio, contenente gli atti del processo come documenti informatici, ovvero le copie informatiche dei medesimi atti, qualora siano stati depositati su supporto cartaceo;
i) soggetti abilitati: tutti i soggetti abilitati all'utilizzo dei servizi di consultazione di informazioni e trasmissione di documenti informatici relativi al processo. In particolare si intende per:
1.1. soggetti abilitati esterni privati: i difensori delle parti private, gli avvocati iscritti negli elenchi speciali, gli esperti e gli ausiliari del giudice;
1.2. soggetti abilitati esterni pubblici: gli avvocati, i procuratori dello Stato e gli altri dipendenti di amministrazioni statali;
1.3. soggetti abilitati esterni: i soggetti abilitati esterni privati e i soggetti abilitati esterni pubblici;
1.4. soggetti abilitati interni: i magistrati, il personale degli uffici giudiziari e degli UNEP;
j) casella di posta elettronica certificata per il processo telematico (CPECPT): indirizzo elettronico, per il processo telematico, dei soggetti abilitati.
3. Gestore centrale.
1. Il gestore centrale è il punto unico di interazione, a livello nazionale, tra il SICI ed i soggetti abilitati esterni.
2. Il gestore centrale è attivo presso il Ministero della giustizia.
4. Gestore locale.
1. Il gestore locale è parte del sistema informatico dell'ufficio giudiziario e dell'UNEP, come definito nel *decreto ministeriale 24 maggio 2001*, e rispetta i requisiti tecnici ed organizzativi definiti in tale àmbito.
2. I gestori locali sono attivi presso gli uffici giudiziari e gli UNEP.
5. Sistemi informatici di gestione della cancelleria e dell'UNEP.
1. Il sistema informatico di gestione delle cancellerie civili è costituito dall'infrastruttura hardware e software di gestione dei registri e dei fascicoli informatici.
2. Il sistema informatico di gestione degli UNEP è costituito dall'infrastruttura hardware e software per la gestione delle notifiche.
6. Punto di accesso.
1. I soggetti abilitati esterni accedono al SICI tramite un punto di accesso, che può essere attivato esclusivamente dai soggetti pubblici, di cui al comma 5, e dai soggetti privati, di cui al comma 6. Ciascun soggetto può avvalersi di un solo punto di accesso.
2. I punti di accesso forniscono un'adeguata qualità dei servizi, dei processi informatici e dei relativi prodotti, idonea a garantire la sicurezza del sistema ed a non comprometterne i livelli di servizio, nel rispetto dei requisiti tecnici di cui all'art. 30.
3. La violazione, da parte di un punto di accesso, dei livelli di sicurezza e di servizio, comporta la sospensione ad erogare i servizi fino al ripristino di tali livelli.
4. Il Ministero della giustizia dispone ispezioni tecniche, anche a campione, per verificare l'attuazione delle prescrizioni di sicurezza.
5. I soggetti pubblici, che possono attivare e gestire uno o più punti di accesso, sono:

a) i consigli dell'ordine degli avvocati, ciascuno limitatamente ai propri iscritti;
b) il Consiglio nazionale forense, limitatamente ai propri iscritti e agli iscritti dei consigli dell'ordine degli avvocati;
c) il Consiglio nazionale del notariato, limitatamente ai propri iscritti;
d) l'Avvocatura dello Stato, le amministrazioni statali o equiparate, e gli enti pubblici, limitatamente ai loro iscritti e dipendenti;
e) il Ministero della giustizia, per i soggetti abilitati interni e in via residuale, ove sussistano oggettive difficoltà per l'attivazione del servizio da parte dei soggetti di cui ai punti *a*) e *b*);
f) il Ministero della giustizia, in via residuale, ove sussistano oggettive difficoltà per l'attivazione del servizio da parte dei soggetti di cui al comma 6, al solo fine di garantire l'accesso agli esperti e ausiliari del giudice.
6. I soggetti privati, che attivano e gestiscono un punto di accesso, hanno i seguenti requisiti:
a) forma di società per azioni;
b) capitale sociale e requisiti di onorabilità di cui al *decreto legislativo 1° settembre 1993, n. 385*, art. 25, comma 1.
7. Certificazione dei difensori.
1. La certificazione del difensore è svolta dal punto di accesso, qualora questo sia gestito da un Consiglio dell'ordine degli avvocati o dal Consiglio nazionale forense, oppure dal gestore centrale sulla base di copia dell'albo fornita al Ministero della giustizia e dai consigli dell'ordine degli avvocati e dal Consiglio nazionale forense.
2. L'aggiornamento della copia dell'albo avviene entro 72 ore dalla comunicazione, dei provvedimenti di pertinenza, all'interessato.
3. Il Consiglio nazionale forense compie il servizio di certificazione dei difensori per i propri iscritti o, per gli iscritti dei consigli dell'ordine, su delega di questi ultimi.
8. Accesso dei soggetti abilitati esterni privati.
1. Per il difensore delle parti è necessaria, ai fini dell'accesso al SICI, l'autenticazione presso il punto di accesso di cui al capo quarto e la certificazione di cui all'art. 7.
2. Il SICI consente al difensore l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui è costituito e permette, negli altri casi, l'acquisizione delle informazioni necessarie per la costituzione in giudizio.
3. In caso di delega, rilasciata ai sensi dell'art. 9, regio decreto legislativo 27 novembre 1933, n. 1578, il SICI consente all'avvocato delegato l'accesso alle informazioni contenute nei fascicoli dei procedimenti patrocinati dall'avvocato delegante, previa comunicazione, a cura di parte, di copia della delega stessa al responsabile dell'ufficio giudiziario, che provvede ai conseguenti adempimenti. L'accesso è consentito fino alla comunicazione della revoca della delega.
4. La delega, sottoscritta con firma digitale, è rilasciata in conformità al modello previsto dall'art. 56.
5. Gli esperti e gli ausiliari del giudice accedono al SICI nel limite dell'incarico ricevuto e della autorizzazione, concessa dal giudice, alla consultazione e alla copia degli atti.
6. A seguito dell'autenticazione, viene trasmesso al gestore centrale il codice fiscale del soggetto abilitato esterno privato.
9. Accesso dei soggetti abilitati esterni pubblici.
1. Il punto di accesso autentica il soggetto abilitato esterno pubblico e trasmette il relativo codice fiscale al gestore centrale.
2. I dati, di cui al comma 1, sono utilizzati per individuare i privilegi di accesso alle informazioni contenute nel SICI.
3. Il SICI consente agli avvocati e procuratori dello Stato l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui è parte una pubblica amministrazione.
10. Accesso dei soggetti abilitati interni.
1. I soggetti abilitati interni accedono al SICI attraverso la rete unica della giustizia (RUG) e attraverso il punto di accesso del Ministero della giustizia.
Capo II - Gestione della posta elettronica
11. Casella di posta elettronica certificata del processo telematico.
1. I soggetti abilitati esterni, per utilizzare i servizi di trasmissione telematica dei documenti informatici, dispongono di un indirizzo elettronico e della relativa casella di posta elettronica, CPECPT, forniti e gestiti dal punto di accesso, nel rispetto dei requisiti di cui all'art. 12.
2. Ogni indirizzo elettronico, come definito nel *decreto del Presidente della Repubblica 13 febbraio 2001, n. 123*, corrisponde ad una CPECPT.

3. Ad ogni soggetto, che interagisce per via telematica con il SICI, corrisponde un solo indirizzo elettronico.
4. Ogni CPECPT è abilitata a ricevere messaggi provenienti unicamente da altri punti di accesso e dal gestore centrale.
12. Requisiti del servizio di gestione della CPECPT.
1. La CPECPT garantisce la ricezione dei messaggi e la loro disponibilità per trenta giorni, successivamente il messaggio è archiviato e sostituito da un avviso contenente i seguenti dati: identificativo univoco del messaggio, mittente, data, ora e minuti di arrivo.
2. Il servizio di posta elettronica certificata restituisce al mittente una ricevuta breve di avvenuta consegna per ogni documento informatico reso disponibile al destinatario, cui è associata l'attestazione temporale di cui all'art. 45.
3. Salvo quanto previsto nel presente decreto e nell'allegato *B*, la posta certificata del processo telematico si conforma alle linee guida stabilite dal Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA).
4. L'avviso di cui al comma 1 è conservato, presso il punto d'accesso, per un periodo non inferiore a cinque anni.
13. Registro generale degli indirizzi elettronici.
1. Il registro generale degli indirizzi elettronici, attivo presso il gestore centrale, contiene l'elenco di tutti gli indirizzi elettronici attivati dai punti di accesso.
2. Il registro generale degli indirizzi elettronici è accessibile a tutti i soggetti abilitati, secondo le modalità previste dall'art. 19.
3. All'indirizzo elettronico delle persone fisiche, sono associate le seguenti informazioni:
a) nome e cognome;
b) luogo e data di nascita;
c) codice fiscale;
d) data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;
e) residenza;
f) domicilio;
g) stato dell'indirizzo: attivo, non attivo;
h) certificato digitale relativo alla chiave pubblica, da utilizzare per la cifratura;
i) consiglio dell'ordine o ente di appartenenza;
j) stato del difensore: attivo, non attivo.
4. All'indirizzo elettronico degli enti collettivi, siano essi non riconosciuti ovvero persone giuridiche, sono associate le seguenti informazioni:
a) denominazione sociale;
b) codice fiscale;
c) data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;
d) sede legale;
e) certificato digitale relativo alla chiave pubblica da utilizzare per la cifratura;
f) stato dell'indirizzo: attivo, non attivo.

14. Registrazione dei soggetti abilitati esterni al SICI.
1. L'accesso al SICI e la casella di posta elettronica si ottengono previa registrazione presso un punto di accesso.
2. La registrazione si ottiene con richiesta scritta, che il punto d'accesso conserva per almeno dieci anni.
3. Con la registrazione, il punto di accesso acquisisce i dati di cui all'art. 13, commi 3 e 4, e verifica l'identità del richiedente ed il relativo codice fiscale.
4. I difensori delle parti presentano, all'atto della registrazione, un certificato, rilasciato in data non anteriore a venti giorni, in cui il consiglio dell'ordine di appartenenza attesta l'iscrizione all'albo, all'albo speciale, al registro dei praticanti abilitati, oppure la qualifica che legittima all'esercizio della difesa e l'assenza di cause ostative allo svolgimento dell'attività difensiva.
5. Gli esperti e gli ausiliari del giudice presentano, all'atto della registrazione, il certificato della iscrizione all'albo dei consulenti tecnici o copia della nomina da parte del giudice dalla quale risulta che l'incarico non è esaurito.
6. Al momento della registrazione, i soggetti abilitati esterni comunicano al punto di accesso le seguenti informazioni:
a) nome e cognome;
b) luogo e data di nascita;

c) codice fiscale;
d) residenza;
e) domicilio;
f) certificato digitale, relativo alla chiave pubblica, per la cifratura;
g) consiglio dell'ordine di appartenenza.
I soggetti abilitati esterni comunicano al punto di accesso ogni variazione delle informazioni di cui alle lettere *d*), *e*), *f*) e *g*).
7. Le informazioni di cui al comma 6, unitamente alla qualità di difensore delle parti, di esperto o ausiliario del giudice, ed all'indirizzo elettronico assegnato e ad eventuali variazioni del suo stato, sono trasmesse dal punto di accesso al gestore centrale e, per i difensori delle parti, al consiglio dell'ordine di appartenenza.
15. Obbligo di informazione.
1. I punti di accesso informano i titolari di indirizzi elettronici degli obblighi assunti in relazione al servizio offerto.
16. Registro degli indirizzi elettronici del punto di accesso.
1. Il punto di accesso attiva un registro degli indirizzi elettronici che contiene l'elenco di tutti gli indirizzi elettronici emessi, revocati o sospesi dal punto di accesso.
2. Ad ogni indirizzo elettronico di persona fisica sono associate le informazioni di cui all'art. 13, comma 3.
3. L'indirizzo elettronico di enti collettivi, siano essi non riconosciuti ovvero persone giuridiche, associa le informazioni di cui all'art. 13, comma 4.
4. Il difensore comunica al consiglio dell'ordine di appartenenza il proprio indirizzo elettronico, relativo alla CPECPT rilasciata dal punto di accesso, unitamente al proprio codice fiscale e ai dati identificativi del punto di accesso.
5. Il difensore delle parti, l'esperto o l'ausiliario del giudice comunica alla cancelleria competente il proprio indirizzo elettronico, relativo alla CPECPT rilasciata dal punto di accesso.
6. Il registro degli indirizzi elettronici è accessibile a tutti i soggetti abilitati, secondo le modalità previste dall'art. 19.
7. Per i soggetti abilitati esterni pubblici, ciascun punto di accesso comunica al Ministero della giustizia, per via telematica, tutte le informazioni di cui all'art. 13, commi 3 e 4, ed ogni loro variazione, al fine dell'inserimento nel registro generale degli indirizzi elettronici.
17. Comunicazioni dei consigli dell'ordine degli avvocati e del Consiglio nazionale forense.
1. Al fine dell'inserimento nei registri degli indirizzi elettronici, i consigli dell'ordine degli avvocati e il Consiglio nazionale forense comunicano al Ministero della giustizia ed ai punti di accesso di riferimento, le seguenti informazioni e le loro variazioni, per via telematica, relative ai difensori:
a) nome e cognome;
b) luogo e data di nascita;
c) codice fiscale;
d) domicilio;
e) indirizzo elettronico, dichiarato e fornito dal punto di accesso;
f) data, ora e minuti dell'ultima variazione dell'indirizzo elettronico;
g) stato dell'indirizzo: attivo, sospeso, non attivo;
h) dati identificativi del punto di accesso che fornisce il servizio di posta elettronica;
i) stato del difensore: attivo, sospeso, cancellato, radiato; con indicazione di inizio efficacia del provvedimento e di fine efficacia nell'ipotesi di provvedimento temporaneo.
2. La comunicazione di cui al comma 1 è sottoscritta, con firma digitale, dal presidente del consiglio dell'ordine ovvero del Consiglio nazionale forense, o da un loro delegato.
3. La comunicazione di cui al comma 1 è strutturata in linguaggio XML, secondo il formato definito nel decreto ministeriale di cui all'art. 52.
18. Requisiti tecnici dei registri degli indirizzi elettronici.
1. Il gestore centrale ed i punti di accesso rendono disponibile una copia operativa dei propri registri degli indirizzi elettronici e mantengono l'originale inaccessibile dall'esterno.
2. Il gestore centrale ed i punti di accesso garantiscono la conformità tra la copia operativa e l'originale dei propri registri e risolvono tempestivamente qualsiasi difformità, registrandola in un apposito giornale di controllo.
3. Le operazioni che modificano il contenuto dei registri sono consentite unicamente al personale espressamente autorizzato e sono registrate in un apposito giornale di controllo.

4. La data, l'ora e i minuti, iniziali e finali, di ogni intervallo di tempo nel quale i registri non risultano accessibili dall'esterno, oppure sono indisponibili in una loro funzionalità, sono registrate in un apposito giornale di controllo.
5. Almeno una copia dei registri è conservata in locali di sicurezza, ubicati in luoghi diversi da quelli ove sono custoditi gli originali.
19. Modalità di accesso ai registri degli indirizzi elettronici.
1. L'accesso ai registri degli indirizzi elettronici avviene secondo una modalità compatibile con il protocollo LDAP, definito nella specifica pubblica RFC 1777 e successive modificazioni.
2. Il gestore centrale dell'accesso e i punti di accesso possono fornire modalità di accesso al proprio registro aggiuntive, rispetto a quella prevista dal comma 1.
3. La struttura LDAP è specificata nei decreti ministeriali di cui all'art. 62, comma 2.
Capo III - Attività del SICI
20. Funzionamento e gestione del SICI.
1. La direzione generale per i sistemi informativi automatizzati del Ministero della giustizia (DGSIA) cura il funzionamento e la gestione del gestore centrale.
2. Il coordinamento interdistrettuale dei sistemi informativi automatizzati (CISIA) cura, attraverso l'amministratore di sistema, il funzionamento del gestore locale degli uffici di competenza.
3. Il dirigente amministrativo dell'ufficio giudiziario e dell'UNEP curano e sono responsabili, per l'ufficio di propria competenza, della consistenza dei dati.
21. Attività del gestore centrale.
1. Il gestore centrale fornisce il servizio di consultazione del SICI e il servizio di trasmissione telematica degli atti. I soggetti abilitati esterni accedono ai servizi del gestore centrale esclusivamente attraverso il proprio punto di accesso.
2. Il gestore centrale è connesso ai punti di accesso mediante canali sicuri.
3. Nelle comunicazioni o notificazioni al difensore, il gestore centrale controlla, mediante il registro generale degli indirizzi elettronici, la certificazione del difensore. In caso di esito negativo del controllo, il gestore centrale inoltra la comunicazione o notifica, e trasmette all'ufficio giudiziario o all'UNEP un messaggio contenente l'esito del controllo.
4. Il gestore centrale associa automaticamente, ad ogni documento informatico pervenuto da un punto di accesso, una attestazione temporale della ricezione del documento informatico, contenente data, ora e minuti, che è inserita in un messaggio inviato all'indirizzo elettronico del mittente.
5. Il gestore centrale associa automaticamente, ad ogni ricevuta breve di avvenuta consegna pervenuta da un punto di accesso, una attestazione temporale, comprensiva di data, ora e minuti di ricezione del relativo documento informatico da parte del destinatario, e trasmette questi dati al gestore locale dell'ufficio giudiziario competente.
6. Il gestore centrale utilizza, per gli adempimenti di cui ai commi 4 e 5, un servizio di attestazione temporale basato, con una differenza non superiore ad un minuto primo, sulla scala di tempo UTC (IEN), determinata ai sensi dell'art. 3, comma 1, della *legge 11 agosto 1991, n. 273*.
7. Il gestore centrale verifica l'assenza di virus informatici in ogni messaggio, in arrivo e in partenza.
8. Il gestore centrale, se riceve un messaggio privo dei dati necessari all'instradamento verso l'ufficio giudiziario o l'UNEP, genera e invia automaticamente al mittente un messaggio di errore, contenente l'avviso del rifiuto del messaggio e l'indicazione degli elementi mancanti.
9. Il gestore centrale inoltra automaticamente tutti i documenti informatici provenienti dall'esterno del SICI e diretti verso il gestore locale dell'ufficio giudiziario o dell'UNEP, ed associa la attestazione temporale.
10. Il gestore centrale fornisce un servizio di inoltro automatico di tutti i documenti informatici ricevuti dall'interno del SICI verso l'indirizzo elettronico di destinazione.
11. Il gestore centrale fornisce il servizio di conservazione di tutti i messaggi inviati e ricevuti, associati alle relative attestazioni temporali, con le modalità previste dalla Del. 19 febbraio 2004, n. 11 del CNIPA. I supporti sono inviati, con periodicità mensile, ad un apposito centro di conservazione presso il Centro di gestione centralizzata del Ministero della giustizia, che ne assicura la conservazione per un periodo non inferiore a cinque anni.
12. Il gestore centrale esegue la certificazione del difensore, qualora non sia già stata compiuta dal punto d'accesso.
13. Il gestore centrale fornisce un servizio per verificare lo stato delle notifiche e delle relative ricevute brevi di avvenuta consegna.
22. Attività del gestore locale.

1. Il gestore locale fornisce il servizio di consultazione del sistema informatico dell'ufficio giudiziario, per i soggetti abilitati, collegati attraverso il gestore centrale.
2. Il gestore locale, mediante il sistema informatico di gestione della cancelleria, fornisce il servizio di consultazione, nei limiti dei privilegi di accesso dell'utente.
3. Il gestore locale trasmette i documenti tra i sistemi informatici dell'ufficio giudiziario o dell'UNEP ed il gestore centrale.
4. Il gestore locale fornisce una verifica della ricezione di tutti i documenti informatici ricevuti dal gestore centrale e delle relative attestazioni temporali.
5. Il gestore locale decifra i messaggi crittografati ricevuti, secondo le regole previste all'art. 42.
6. Il gestore locale cifra, con le modalità di cui all'art. 43, i documenti in uscita, facenti parte del fascicolo informatico, quando sono destinati a soggetti abilitati esterni.
7. Il gestore locale verifica automaticamente, con il controllo della firma digitale, l'autenticità e l'integrità di ogni documento informatico ricevuto.
8. Il gestore locale verifica il rispetto dei formati e l'assenza di virus.
9. Il gestore locale rende disponibile il documento ricevuto al sistema informatico di gestione delle cancellerie civili o dell'UNEP, associandovi le informazioni dell'attività di verifica di cui al comma 8, per valutarne la ricevibilità.

23. Attività del sistema informatico di gestione della cancelleria.

1. Il sistema informatico di gestione delle cancellerie civili cura l'accettazione del documento ricevuto aggiornando il relativo registro ed il fascicolo informatico.
2. Il sistema informatico di gestione delle cancellerie civili invia, tramite il gestore locale ed il gestore centrale, all'indirizzo elettronico del mittente, una comunicazione di accettazione del documento informatico da parte della cancelleria oppure i motivi della mancata accettazione. La comunicazione contiene, se possibile, il numero di iscrizione a ruolo.

24. Attività del sistema informatico di gestione dell'UNEP.

1. Il sistema informatico di gestione degli UNEP acquisisce i documenti informatici da notificare, procede alla loro notifica e li restituisce con la relata di notifica.

25. Orario di disponibilità dei servizi.

1. Il gestore centrale ed i gestori locali garantiscono la disponibilità del servizio, nei giorni feriali, dalle ore otto alle ore ventitrè, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.

26. Requisiti tecnici di sicurezza.

1. Al gestore centrale si applicano le regole di sicurezza stabilite per il SICI e per la RUG.
2. Per il gestore locale e per il fascicolo informatico si applicano le norme sulla sicurezza previste dal *D.M. 24 maggio 2001* del Ministero della giustizia.

27. Requisiti tecnici relativi all'infrastruttura di comunicazione.

1. Il gestore centrale ed i gestori locali comunicano, tra loro, esclusivamente mediante la RUG.
2. Il gestore centrale utilizza l'infrastruttura tecnologica resa disponibile nell'àmbito della rete unitaria della pubblica amministrazione (RUPA) per le comunicazioni con l'esterno del dominio giustizia.

Capo IV - Accesso al SICI

28. Funzionamento e gestione del punto di accesso.

1. Il funzionamento e la gestione dei punti di accesso è a carico dei soggetti pubblici o privati, in possesso dei requisiti di cui all'art. 6.

29. Funzionalità del punto di accesso.

1. Il punto di accesso fornisce ai soggetti abilitati esterni i servizi di consultazione del SICI e di trasmissione telematica degli atti.
2. Il punto di accesso fornisce il servizio di autenticazione dei soggetti abilitati, per l'accesso al SICI. Il punto di accesso, gestito dal consiglio dell'ordine degli avvocati di appartenenza o dal Consiglio nazionale forense, con l'autenticazione del difensore, esegue la certificazione di cui all'art. 7.
3. La comunicazione tra la postazione informatica del soggetto abilitato esterno e il punto di accesso avviene mediante canale sicuro.
4. Il punto di accesso mantiene in linea i documenti informatici inviati fino a quando non riceve un avviso di consegna dal gestore centrale o dal punto di accesso di destinazione.
5. Il punto di accesso fornisce il servizio di ricezione, inviando, in risposta ad ogni documento informatico ricevuto dal gestore centrale o da un altro punto di accesso, una ricevuta breve di avvenuta consegna.
6. Il punto di accesso verifica l'assenza di virus informatici in ogni messaggio in arrivo e in partenza.

7. Il punto di accesso garantisce, per un periodo non inferiore a cinque anni, la conservazione di tutti i messaggi inviati e ricevuti.
8. Il punto di accesso fornisce il servizio di distribuzione del software, fornito come prototipo dal Ministero della giustizia, per la redazione dei documenti informatici in formato XML.
30. Requisiti tecnici del punto di accesso.
1. L'autenticazione dei soggetti abilitati esterni avviene secondo le specifiche previste dalla carta nazionale dei servizi.
2. I punti di accesso stabiliscono le connessioni con il gestore centrale esclusivamente mediante un collegamento diretto alla RUPA, autorizzato dal CNIPA.
3. Ciascun punto di accesso stabilisce con il gestore centrale un canale sicuro di comunicazione, che consente la reciproca autenticazione e riservatezza.
4. Il punto di accesso garantisce un livello di disponibilità del servizio pari al 99,5 per cento, su base quadrimestrale, nei giorni feriali, dalle ore otto alle ore ventidue, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.
5. Le procedure per la fornitura dei servizi attuate dal punto di accesso sono dettagliatamente documentate sul manuale operativo, previsto dall'art. 33.
6. Tutte le azioni e le procedure di sicurezza attivate dal punto di accesso sono dettagliatamente documentate nel piano per la sicurezza, previsto dall'art. 34.
7. La frequenza di salvataggio dei dati è almeno giornaliera.
8. Gli eventi significativi nel funzionamento del punto di accesso, sono registrati sul giornale di controllo, di cui all'art. 35.
9. I canali di autenticazione del presente regolamento sono in SSL versione 3, con chiave a 1024 bit.
31. Elenco pubblico dei punti di accesso.
1. L'elenco pubblico dei punti di accesso, attivo presso il Ministero della giustizia, comprende le seguenti informazioni:
a) identificativo del punto di accesso;
b) sede legale del soggetto titolare del punto di accesso;
c) nome secondo lo standard X.500;
d) indirizzo Internet;
e) dati relativi al legale rappresentante del punto di accesso o a un suo delegato, comprendenti: nome, cognome, codice fiscale, indirizzo elettronico, numero di telefono e di fax;
f) elenco dei numeri telefonici di accesso;
g) manuale operativo;
h) data di cessazione dell'attività.
32. Iscrizione nell'elenco pubblico dei punti di accesso.
1. Il soggetto che intende costituire un punto di accesso inoltra, alla DGSIA, domanda di iscrizione nell'elenco pubblico dei punti di accesso.
2. Alla domanda sono allegate le dichiarazioni di:
a) possesso dei requisiti di cui all'art. 6;
b) attestazione di affidabilità organizzativa e tecnica necessaria per svolgere il servizio di punto di accesso;
c) attestazione relativa all'impiego di personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti;
d) obbligo di fornirsi di: manuale operativo, piano per la sicurezza e giornale di controllo, secondo quanto previsto dagli articoli 33, 34 e 35;
e) obbligo di garantire la sicurezza e l'integrità del servizio e dei dati di propria competenza;
f) obbligo di compiere il processo di autenticazione dei soggetti abilitati ad esso afferenti, su mandato del Ministero della giustizia, conformemente all'art. 30, comma 1;
g) obbligo di comunicare, al Ministero della giustizia, la data di cessazione del servizio, con preavviso di sei mesi;
h) informazione dei dati di cui all'art. 31.
3. Il Ministero della giustizia decide sulla domanda, con provvedimento motivato, anche sulla base di apposite verifiche, effettuabili anche da personale esterno all'Amministrazione, da questa delegato, con costi a carico del richiedente.
4. Con il provvedimento di cui al comma 3, il Ministero della giustizia delega la responsabilità del processo di autenticazione dei soggetti abilitati esterni al punto di accesso.

5. Il Ministero della giustizia può verificare l'adempimento degli obblighi assunti da parte del gestore del punto di accesso, di propria iniziativa oppure su segnalazione. In caso di violazione si applicano le disposizioni di cui all'art. 6, comma 3.

33. Manuale operativo.

1. Il punto di accesso utilizza un manuale operativo in cui sono definite le procedure applicate per effetto del presente decreto.
2. Il manuale operativo è pubblicato a cura del punto di accesso, per la consultazione in via telematica.
3. Il manuale operativo contiene almeno le seguenti informazioni:
a) dati identificativi del punto di accesso e del relativo gestore;
b) dati identificativi della versione del manuale operativo;
c) responsabile del manuale operativo;
d) definizione degli obblighi del titolare del punto di accesso e di coloro che vi accedono per l'utilizzo dei servizi;
e) definizione delle responsabilità e delle eventuali limitazioni agli indennizzi;
f) tariffe;
g) modalità di autenticazione, registrazione e gestione degli utenti;
h) modalità di attivazione e gestione degli indirizzi elettronici;
i) modalità di gestione del registro degli indirizzi elettronici;
j) modalità di accesso al registro degli indirizzi elettronici;
k) politiche e procedure di sicurezza.

34. Piano per la sicurezza.

1. Il punto di accesso individua ed iscrive, nel giornale di controllo, il responsabile per la sicurezza.
2. Il responsabile di cui al comma 1 definisce il piano per la sicurezza che contiene almeno i seguenti elementi:
a) struttura generale, modalità operativa e struttura logistica dell'organizzazione;
b) descrizione dell'infrastruttura di protezione per ciascun immobile rilevante ai fini della sicurezza;
c) collocazione dei servizi e degli uffici negli immobili dell'organizzazione;
d) elenco del personale e sua distribuzione negli uffici;
e) ripartizione e definizione delle responsabilità;
f) descrizione delle procedure utilizzate nell'attività di attivazione delle utenze e, limitatamente ai punti di accesso, di rilascio di indirizzi elettronici;
g) descrizione dei dispositivi installati;
h) descrizione dei flussi di dati;
i) procedura di gestione delle copie di sicurezza dei dati;
j) procedura di gestione dei disastri;
k) analisi dei rischi;
l) descrizione delle contromisure;
m) specificazione dei controlli.
3. Il piano per la sicurezza è conforme a quanto previsto dal *decreto legislativo 30 giugno 2003, n. 196*, e può essere adottato unitamente al documento programmatico per la sicurezza previsto dall'art. 34, comma 1, lettera *g*), del medesimo decreto legislativo.

35. Giornale di controllo.

1. Il punto di accesso attiva il giornale di controllo, contenente l'insieme delle registrazioni effettuate automaticamente allorché si verificano le condizioni previste dal presente decreto.
2. Le registrazioni possono essere effettuate in modo indipendente, anche su distinti supporti e di diverso tipo.
3. La registrazione associa la data, l'ora e i minuti in cui è effettuata.
4. Il giornale di controllo è tenuto in modo da garantire l'autenticità delle annotazioni e da consentire la ricostruzione accurata di tutti gli eventi rilevanti per la sicurezza.
5. L'integrità del giornale di controllo è verificata con frequenza almeno mensile.
6. Le registrazioni contenute nel giornale di controllo sono archiviate con le modalità previste dal presente decreto e conservate per un periodo non inferiore a cinque anni.

36. Postazioni di lavoro dei soggetti abilitati esterni.

1. La postazione di lavoro dei soggetti abilitati esterni è l'insieme delle risorse hardware, software e di rete da loro utilizzate direttamente per la formazione dei documenti informatici, per l'inoltro e la ricezione dei messaggi e per la consultazione del SICI.

2. La postazione di lavoro dei soggetti abilitati esterni è dotata dell'hardware e del software necessario alla gestione della firma digitale su smartcard, e all'autenticazione nei confronti del punto di accesso, secondo le caratteristiche tecniche della carta nazionale dei servizi.
3. La postazione di lavoro dei soggetti abilitati esterni è dotata di software idoneo a verificare l'assenza di virus informatici in ogni messaggio in arrivo e in partenza.

Capo V - Trasmissione di documenti informatici tra il SICI ed entità esterne

37. Principi normativi.

1. Nella trasmissione di documenti informatici nell'àmbito del processo civile, trovano applicazione tutte le prescrizioni contenute nel *decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*, nel *decreto legislativo 23 gennaio 2002, n. 10*, e successive modificazioni.
2. I documenti informatici prodotti nel processo civile sono sottoscritti con firma digitale, nei casi previsti dall'art. 4, comma 3, del *decreto del Presidente della Repubblica 13 febbraio 2001, n. 123*.

38. Ricezione del documento informatico.

1. Il documento informatico inviato da un soggetto abilitato esterno è ricevuto dal SICI nel momento in cui il gestore centrale lo accetta e associa l'attestazione temporale di cui all'art. 21, comma 4.
2. Il documento informatico inviato da un soggetto abilitato interno è ricevuto, dal soggetto abilitato esterno, nel momento in cui il gestore centrale riceve la ricevuta breve di avvenuta consegna relativa al documento e associa l'attestazione temporale di cui all'art. 21, comma 5.

39. Orario dei servizi telematici di cancelleria.

1. Il SICI fornisce i servizi telematici di cancelleria, nei giorni feriali, dalle ore otto alle ore ventidue, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentuno dicembre.

40. Iscrizione a ruolo generale.

1. Il sistema informatico dell'ufficio giudiziario invia al difensore, che iscrive la causa a ruolo per via telematica, una comunicazione, recante il numero di ruolo del procedimento assegnato dall'ufficio.

41. Dimensione del messaggio.

1. La dimensione massima del messaggio è di 10 Mb.

42. Crittografia del messaggio.

1. Al fine della riservatezza del documento da trasmettere, il soggetto abilitato esterno utilizza un meccanismo di crittografia basato sulla chiave pubblica del gestore locale cui è destinato il messaggio.
2. Le caratteristiche tecniche specifiche della crittografia dei documenti sono definite nell'allegato *A* del presente decreto.
3. Le chiavi pubbliche dei gestori locali sono pubblicate in un registro del gestore centrale dell'accesso.
4. Il registro di cui al comma 3 è accessibile in modalità LDAP.

43. Trasmissione e consultazione dei fascicoli.

1. Nel caso di richiesta di trasmissione o di consultazione, totale o parziale, di un fascicolo, il gestore locale, per garantire la riservatezza della comunicazione, utilizza un meccanismo di crittografia basato sulla chiave pubblica di cifratura del soggetto abilitato esterno di destinazione.
2. Nel caso di richiesta di copia conforme del fascicolo, totale o parziale, il cancelliere ne attesta la conformità all'originale sottoscrivendola con la propria firma digitale.
3. Le chiavi pubbliche dei soggetti abilitati esterni sono disponibili nel registro generale degli indirizzi di cui all'art. 13.
4. Le caratteristiche tecniche specifiche della crittografia dei documenti sono definite nell'allegato *A*, del presente decreto.

44. Trasmissione delle sentenze.

1. L'originale della sentenza, redatta in formato elettronico dal giudice estensore o, ai sensi dell'art. 119 delle norme di attuazione del codice di procedura civile, dal cancelliere o dal dattilografo da questi incaricato, è sottoscritta con firma digitale dall'estensore, previa verifica della conformità dell'originale alla minuta.
2. In caso di giudice collegiale, l'originale della sentenza è sottoscritto con firma digitale anche dal presidente e, a tal fine, la sentenza gli è trasmessa, in formato elettronico, dal giudice estensore o dal cancelliere.
3. Il cancelliere attesta il deposito della sentenza apponendo la data e sottoscrivendo la sentenza con la propria firma digitale.

45. Comunicazioni e notificazioni.

1. La comunicazione per via telematica di documenti informatici dall'ufficio giudiziario ad un soggetto abilitato esterno avviene mediante inoltro del documento dal gestore locale al gestore centrale, che lo invia alla CPECPT del destinatario.

2. La notificazione telematica di documenti informatici tra difensori avviene, ove sussistano i presupposti di cui alla *legge 21 gennaio 1994, n. 53*, mediante inoltro del documento dal punto di accesso del mittente alla CPECPT del destinatario. A tale scopo il punto di accesso trasmette il messaggio con il documento da notificare al gestore centrale che, a sua volta, inoltra il messaggio ricevuto al punto di accesso di destinazione.
3. Le richieste di un'attività di notifica telematica da parte di un ufficio giudiziario sono inoltrate, mediante la RUG, al sistema informatico dell'UNEP. Le richieste dei difensori sono inoltrate all'UNEP per il tramite del punto di accesso del mittente e del gestore centrale, nel rispetto dei requisiti dei documenti informatici provenienti dall'esterno. La notificazione di documenti informatici da parte dell'UNEP rispetta i requisiti richiesti per la comunicazione da ufficio giudiziario verso soggetti abilitati esterni.
4. Il sistema informatico dell'UNEP, eseguita la notifica, trasmette per via telematica, a chi ha richiesto il servizio, il documento informatico con la relata di notifica, costituita dalla ricevuta elettronica, sottoscritta dall'ufficiale giudiziario con firma digitale.
5. Nell'ipotesi di cui all'art. 6, comma 3, del *decreto del Presidente della Repubblica 13 febbraio 2001, n. 123*, l'ufficiale giudiziario provvede a notificare il duplicato del documento informatico, su supporto ottico non riscrivibile.
6. La consegna del documento informatico alla CPECPT del soggetto abilitato esterno è assicurata dai punti di accesso mediante l'invio al mittente di una ricevuta breve di avvenuta consegna.
7. Il gestore centrale, nella trasmissione di documenti informatici dall'ufficio giudiziario ad un soggetto abilitato esterno, associa automaticamente ad ogni ricevuta breve di avvenuta consegna una attestazione temporale contenente data, ora e minuti della ricezione che inoltra al gestore locale per l'inserimento nel fascicolo informatico.
8. Nelle notifiche tra difensori, il gestore centrale, ricevuto dal mittente il messaggio da notificare, associa automaticamente ad esso una prima attestazione temporale, che viene spedita alla CPECPT del mittente e, unitamente al messaggio, alla CPECPT del destinatario. La CPECPT del destinatario, ricevuto il messaggio, invia al gestore centrale la ricevuta breve di avvenuta consegna; il gestore centrale associa a quest'ultima una seconda attestazione temporale, che viene spedita alla CPECPT del destinatario e, unitamente alla ricevuta breve di avvenuta consegna, alla CPECPT del mittente.

Capo VI - Pagamenti

46. Pagamenti.

1. I pagamenti per via telematica, relativi agli atti giudiziari, si effettuano mediante il modello definito dal Ministero dell'economia e delle finanze.
2. Il pagamento può anche avvenire nelle forme di cui all'art. 1 del *decreto del Presidente della Repubblica 1° marzo 2001, n. 126*.
3. Gli estremi del pagamento sono allegati alla nota di iscrizione a ruolo o ad altra istanza inviata all'ufficio giudiziario.
4. Se il pagamento è effettuato a norma del comma 2 e con sistemi non telematici, l'originale cartaceo dell'attestazione di pagamento deve, in ogni caso, essere presentato per la prima udienza.

47. Diritto di copia.

1. Il difensore nella richiesta di copia può chiedere l'indicazione dell'importo del diritto corrispondente che gli è comunicato, senza ritardo, dall'ufficio giudiziario.
2. Alla richiesta di copia è associato un numero identificativo che, in caso di pagamento dei diritti di copia non contestuale, viene evidenziato nel fascicolo informatico per consentire il versamento secondo le modalità previste dal *decreto del Presidente della Repubblica 1° marzo 2001, n. 126*.

48. Registrazione, trascrizione e voltura degli atti.

1. La registrazione, la trascrizione e la voltura degli atti avvengono, in via telematica, nelle forme previste dall'art. 73 del *decreto del Presidente della Repubblica 30 maggio 2002, n. 115*.

49. Pagamento dei diritti di notifica.

1. Il pagamento dei diritti di notifica viene effettuato nelle forme previste dall'art. 46.
2. L'UNEP rende pubblici, attraverso il gestore locale dell'ufficio, gli importi dovuti a titolo di anticipazione. Eseguita la notifica, l'UNEP comunica l'importo definitivo e restituisce il documento informatico notificato previa definizione del conguaglio dovuto dalla parte oppure unitamente al rimborso del maggior importo versato in acconto.

Capo VII - Archiviazione e conservazione delle informazioni

50. Gestione del fascicolo informatico.

1. Il sistema di gestione del fascicolo informatico è la parte del sistema dell'ufficio giudiziario dedicata all'archiviazione e al reperimento di tutti i documenti informatici, prodotti sia all'interno che all'esterno dell'ufficio giudiziario.
2. Il fascicolo informatico contiene i documenti informatici e le relative informazioni quali: allegati, ricevute brevi di avvenuta consegna e attestazioni temporali.
51. Archiviazione e conservazione dei documenti informatici degli uffici giudiziari e degli UNEP.
1. I fascicoli informatici relativi ai procedimenti in corso sono archiviati, per tutta la durata del procedimento, nell'archivio in linea dell'ufficio giudiziario, secondo le modalità previste dal *decreto ministeriale del 24 maggio 2001* e dal *decreto legislativo 30 giugno 2003, n. 196*.
2. I fascicoli informatici relativi ai procedimenti esauriti sono soggetti a conservazione, presso il competente ufficio giudiziario, secondo le modalità previste dalla Del. 19 febbraio 2004, n. 11 del CNIPA, per il periodo previsto dall'art. 41 del *decreto legislativo 22 gennaio 2004, n. 42*, fatte salve le operazioni di scarto ivi previste.
3. I documenti informatici degli UNEP sono soggetti a conservazione, presso il competente ufficio, secondo le modalità e termini di cui al comma 2.
Capo VIII - Standard e modelli di riferimento
52. Formato dei documenti informatici.
1. Gli atti del processo in forma di documenti informatici sono redatti in formato XML, le cui specifiche tecniche sono determinate a norma dell'art. 62, comma 2.
53. Formato dei documenti informatici allegati.
1. I documenti informatici allegati sono privi di elementi attivi, tra cui macro e campi variabili, ed hanno i seguenti formati: .pdf, .rtf, .txt, .jpg, .gif, .tiff, .xml.
2. È consentito l'utilizzo dei formati compressi .zip, .rar. e .arj, purché contenenti file nei formati previsti dal comma precedente.
54. Documenti probatori e allegati non informatici.
1. I documenti probatori e gli allegati depositati in formato non elettronico sono identificati e descritti in una apposita sezione del documento informatico, secondo la definizione del modello DTD (Document Type Definition) e comprendono, per l'individuazione dell'atto di riferimento, i seguenti dati: numero di ruolo della causa, progressivo dell'allegato e indicazione della prima udienza successiva al deposito.
55. Servizio di posta elettronica.
1. Il servizio di posta elettronica utilizzato dal gestore centrale dell'accesso e dai punti di accesso è conforme agli standard dei sistemi di posta elettronica compatibili con il protocollo di trasporto SMTP ed il formato dei messaggi S/MIME.
56. Modelli di documenti informatici prodotti dai difensori.
1. I modelli dei documenti informatici prodotti dai difensori, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:
a) atto introduttivo (citazione, ricorso, ricorso cautelare, ricorso per decreto ingiuntivo);
b) nota di iscrizione a ruolo;
c) comparsa di costituzione e risposta con eventuale domanda riconvenzionale ed eventuale richiesta di rinvio della prima udienza per la chiamata in causa del terzo;
d) deduzioni istruttorie a norma dell'art. 184 del codice di procedura civile;
e) note autorizzate ex art. 183, comma 5, del codice di procedura civile;
f) memorie autorizzate;
g) chiamata in causa del terzo;
h) istanza;
i) reclamo;
j) atti conclusivi (comparsa conclusionale, memoria di replica);
k) atto di pignoramento;
l) atto di intervento nell'esecuzione;
m) osservazioni al progetto di distribuzione;
n) istanza di fallimento;
o) istanza di insinuazione al passivo;
p) ricorso per insinuazione tardiva;
q) ricorso per opposizione allo stato passivo;
r) istanza di ammissione alla procedura di amministrazione controllata;
s) istanza di ammissione alla procedura di concordato preventivo;
t) istanza di concordato fallimentare;
u) dichiarazione di voto nelle procedure di amministrazione controllata o di concordato;

v) delega rilasciata ai sensi dell'art. 9 del regio decreto legislativo 27 novembre 1933, n. 1578.
57. Modelli di documenti informatici prodotti dalla cancelleria.
1. I modelli dei documenti informatici prodotti dalla cancelleria, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:
a) verbale di udienza;
b) biglietto di cancelleria;
c) richiesta di notifica;
d) richiesta di informazione o ordine di esibizione.
58. Modelli di documenti informatici prodotti dal giudice.
1. I modelli dei documenti informatici prodotti dal giudice, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:
a) provvedimento (sentenza, ordinanza, decreto);
b) dispositivo sentenza;
c) verbale di conciliazione.
59. Modelli di documenti informatici prodotti dal consulente tecnico di ufficio.
1. I modelli dei documenti informatici prodotti dal consulente tecnico di ufficio, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi ai seguenti atti:
a) modello generico di consulenza;
b) stima di beni mobili;
c) stima di beni immobili;
d) stima di azienda.
60. Modelli di documenti informatici prodotti dall'UNEP.
1. Il modello dei documenti informatici prodotti dall'UNEP, riportati nei decreti ministeriali di cui all'art. 62, comma 2, sono relativi al seguente atto: relata di notifica.
Capo IX - Disposizioni finali e transitorie
61. Adeguamento delle regole tecnico-operative.
1. Le regole tecnico-operative sono adeguate all'evoluzione scientifica e tecnologica, con cadenza almeno biennale, a decorrere dalla data di entrata in vigore del presente decreto.
62. Disposizioni transitorie.
1. L'attivazione del processo telematico è preceduta da un decreto dirigenziale, che accerta l'installazione e l'idoneità delle attrezzature informatiche, unitamente alla funzionalità dei servizi di comunicazione dei documenti informatici nel singolo ufficio.
2. Le caratteristiche specifiche della strutturazione dei modelli DTD (Document Type Definition) saranno pubblicate, con uno o più decreti ministeriali, entro 180 giorni dalla data di entrata in vigore del presente decreto.
3. Fino all'entrata in vigore delle regole tecniche relative alla carta nazionale dei servizi, l'autenticazione dei soggetti abilitati esterni avviene mediante dispositivo di crittografia contenente al suo interno un certificato di autenticazione e la corrispondente chiave privata protetta da PIN. La chiave privata, lunga almeno 1024 bit e generata all'interno del dispositivo crittografico, non deve essere estraibile dal dispositivo stesso.
4. L'art. 22, comma 6, e l'art. 43, comma 1, hanno efficacia a decorrere da sei mesi dalla data di entrata in vigore del presente decreto.

Il decreto ministeriale 24 maggio 2001 fissa le regole per la tenuta dei registri informatizzati dell'amministrazione della giustizia

NUMERO SCHEDA: 730

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: Privacy

FONTE: MINISTERI

NATURA ATTO: DECRETO MINISTERIALE

Con dec 24 maggio 2001 sono state adottate le "Regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia".
Si ricorda che con d.m. 27 marzo 2000, n. 264 è stato adottato il "Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari".

Si riportano i testi.

D.M. 24 maggio 2001
Regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia.

1. 1. Il presente decreto stabilisce le regole procedurali di cui all'art. 1, comma 1, lettera f), del decreto ministeriale 27 marzo 2000, n. 264, relative ai registri informatizzati tenuti, a cura delle cancellerie o delle segreterie, presso gli uffici giudiziari, ovvero ai registri previsti da codici, da leggi speciali o da regolamenti, comunque connessi all'espletamento delle attribuzioni e dei servizi svolti dall'amministrazione della giustizia.
2. Per le modalità di tenuta informatizzata dei registri e per la sottoscrizione con firma digitale dei documenti informatici si tiene conto anche delle regole tecniche emanate ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
3. Le regole procedurali di cui al comma 1 sono riportate nell'allegato al presente decreto.

Allegato ex art. 1

REGOLE PROCEDURALI PER LA TENUTA DEI REGISTRI INFORMATIZZATI DEGLI UFFICI

Capo I - Definizioni e princìpi generali

Articolo 1
Sistema informativo.

1. Il sistema informativo è definito come l'insieme delle risorse umane, delle regole organizzative, delle risorse hardware e software (applicazioni e dati), dei locali e della documentazione (sia in formato cartaceo, sia elettronico) che, nel loro complesso, consentono di acquisire, memorizzare, elaborare, scambiare e trasmettere informazioni inerenti i registri informatizzati degli uffici.
2. Ai fini delle presenti regole procedurali assumono rilevanza particolare le seguenti componenti del sistema informativo:
a) il sottosistema delle risorse umane, cioè le persone che gestiscono e utilizzano il sistema;
b) il sottosistema dell'infrastruttura logistica, costituito dai locali in cui sono localizzati i sottosistemi di cui alle lettere seguenti;
c) il sottosistema delle postazioni di lavoro, costituito dagli apparati hardware, dal software di base (sistemi operativi) e dal software di accesso alle basi di dati;
d) il sottosistema applicativo, costituito dal software sviluppato specificamente per l'informatizzazione degli uffici nonché dagli apparati hardware, dal software di base (sistemi operativi) e dal software di gestione delle basi di dati;
e) il sottosistema dei dati, costituito dall'insieme delle basi di dati e dei file in cui sono conservati i documenti di pertinenza dell'ufficio;
f) il sottosistema di connessione interna o rete locale, costituito dall'hardware e dal software utilizzati per la connessione delle postazioni di lavoro (cablaggio, apparati di rete attivi e passivi, software di gestione rete, ecc.);
g) il sottosistema di connessione con l'esterno, costituito dall'hardware e dal software utilizzati per la connessione della rete locale con il mondo esterno (firewall, router, modem, linea, ecc.);
h) il sottosistema dei servizi di rete, costituito dall'hardware e dal software che tramite la rete realizzano funzioni tese a facilitare lo svolgimento di operazioni comuni o ripetitive tra utenti e utenti, tra utenti e applicazioni nonché tra applicazioni ed applicazioni (DHCP, DNS, E-MAIL, DMZ, SICAP, ecc.).
3. Le componenti dedicate esclusivamente all'ufficio, specificate al comma 2, lettere c), d), e), insieme con le relative quote di pertinenza dei sottosistemi delle risorse umane e dell'infrastruttura logistica, costituiscono il sistema informativo dell'ufficio.

4. Le risorse condivise, specificate al comma 2, lettere f), g), h), insieme con le relative quote di pertinenza dei sottosistemi delle risorse umane e dell'infrastruttura logistica, costituiscono il sistema informativo di edificio.

Articolo 2
Caratteristiche del sistema informativo.

1. Il sistema informativo soddisfa le seguenti proprietà:
a) disponibilità: le informazioni ed i servizi sono a disposizione degli utenti del sistema, compatibilmente con i livelli di servizio prestabiliti;
b) integrità: le informazioni ed i servizi possono essere creati, modificati o cancellati solo dalle persone autorizzate e secondo modalità predefinite;
c) autenticità: la provenienza dei dati è garantita e asseverata;
d) controllo degli accessi: le informazioni possono essere fruite solo ed esclusivamente dalle persone autorizzate a compiere tale operazione.

Articolo 3
Responsabile della tenuta dei registri.

1. Il dirigente amministrativo dell'ufficio è il responsabile della tenuta dei registri e provvede alla stesura del piano della sicurezza di cui al successivo art. 7, secondo le indicazioni dell'ufficio del responsabile per i sistemi informativi automatizzati (di seguito URSIA), vigilando sulla sua applicazione.

Articolo 4
Amministratore di sistema.

1. L'amministratore di sistema assicura la conduzione operativa del sistema informativo, effettuando tutte le operazioni necessarie a garantire le proprietà di cui all'art. 2.
2. I compiti dell'amministratore di sistema sono svolti da una o più figure professionali del settore della professionalità informatica a seconda delle dimensioni degli uffici e del numero degli edifici.
3. Un unico soggetto può svolgere tali funzioni per più uffici o per più edifici.
4. L'URSIA provvede a designare i soggetti di cui ai commi 2 e 3 del presente articolo e, qualora riguardi un ufficio giudiziario appartenente ad un distretto, lo individua fra gli esperti informatici del competente coordinamento dei sistemi informativi automatizzati (di seguito CISIA); nel caso in cui non siano disponibili tali risorse, si ricorre a tecnici informatici esterni.
5. Nel caso siano stati individuati più soggetti per lo svolgimento delle funzioni di amministratore di sistema, l'URSIA designa il coordinatore.

Articolo 5
Utenti interni ed esterni.

1. L'insieme degli utenti interni è costituito dal personale dell'ufficio abilitato all'accesso al sistema informativo.
2. Gli utenti interni operano secondo le prescrizioni indicate, nel capo V e nel manuale per l'utente di cui all'art. 22, comma 2.
3. L'insieme degli utenti esterni è costituito dai soggetti, non appartenenti al personale dell'ufficio stesso, i quali sono abilitati da norme di legge e di regolamento all'utilizzo dei servizi telematici dell'ufficio.

Capo II - Misure di tipo organizzativo

Articolo 6
Identificazione delle componenti del sistema informativo.

1. È cura del responsabile della tenuta dei registri, con l'ausilio dell'amministratore di sistema, produrre e mantenere aggiornato un dettagliato inventario di tutti gli elementi facenti parte del sistema informativo di sua competenza.
2. Nel caso di più uffici nello stesso edificio i capi degli uffici interessati indicheranno il responsabile della tenuta dei registri che dovrà curare l'inventario delle risorse condivise.
3. L'inventario di cui al comma 1 è aggiornato ogni qualvolta si verifica una variazione qualsiasi nel sistema informativo dell'ufficio o dell'edificio e la sua corrispondenza con la situazione reale è verificata con cadenza almeno trimestrale. In ogni caso, l'inventario è gestito in modo tale da risultare sempre aggiornato e corrispondente alla situazione reale.

Articolo 7
Piano per la sicurezza del sistema informativo dell'ufficio e dell'edificio.

1. Il responsabile della tenuta dei registri, con la collaborazione dell'amministratore di sistema, provvede alla stesura e all'aggiornamento periodico di un piano per la sicurezza del sistema informativo dell'ufficio, secondo gli standard definiti dall'URSIA.
2. Nel caso di più uffici che condividano lo stesso edificio, il piano per la sicurezza è stilato con la collaborazione, per quanto di competenza, dei responsabili della tenuta dei registri dei singoli uffici.
3. Il piano per la sicurezza contiene almeno le seguenti informazioni:
a) inventario delle risorse, di cui all'art. 6;
b) misure adottate per la protezione fisica delle aree e dei locali interessati, di cui al capo III;
c) misure adottate per il controllo degli accessi, di cui agli articoli 8, 13 e 17;
d) misure di monitoraggio del sistema, di cui all'art. 9;
e) misure adottate per garantire l'integrità e la disponibilità dei dati, di cui all'art. 10;
f) misure adottate per garantire la continuità degli applicativi relativi ai registri informatizzati nel caso in cui si verifichi un mal funzionamento dei server interessati;
g) piano di adeguamento degli applicativi, di cui all'art. 19, comma 9;
h) la frequenza e le modalità delle procedure di archiviazione ottica e di copia storica dei dati, coerentemente con le indicazioni di cui all'art. 12 del decreto 27 marzo 2000, n. 264, del Ministro della giustizia.
4. Il piano per la sicurezza contiene indicazioni circa la necessità di avere impianti ridondati e con elevata tolleranza ai guasti.
5. Il piano per la sicurezza prevede misure conformi, per quanto attiene al trattamento dei dati personali, a quanto prescritto dal regolamento di cui all'art. 15, comma 2, della legge 31 dicembre 1996, n. 675.
6. La vigilanza sulla predisposizione e sull'applicazione dei piani di sicurezza è esercitata dai capi degli uffici, secondo le rispettive competenze, avvalendosi anche di un esperto informatico designato dall'URSIA.

Articolo 8
Politica di gestione degli accessi.

1. Ai sensi dell'art. 5 del decreto 27 marzo 2000, n. 264, del Ministro della giustizia la procedura di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo, denominato profilo, rispetto alle risorse del sistema informatico.
2. Attraverso la procedura di autenticazione si individua un insieme di gruppi di utenti a livello di sistema, a livello di database management system ed a livello di applicativo. A ciascun gruppo di utenti è associato uno ed un solo profilo mentre a ciascun utente può essere assegnato uno o più profili.
3. A livello di sistema deve essere definito almeno un gruppo per ciascuna delle figure previste dagli articoli 3, 4 e 5 delle presenti regole procedurali. In corrispondenza di ciascun gruppo è definito un profilo tale da assegnare a ciascun utente appartenente al gruppo solo ed esclusivamente i privilegi di accesso ed utilizzo strettamente necessari per l'espletamento delle attività di propria competenza.
4. Per ciascuna base di dati sono definiti almeno un gruppo amministratori ed un gruppo utenti a livello di database management system.
In corrispondenza di ciascun gruppo è definito un profilo tale da assegnare a ciascun utente appartenente al gruppo solo ed esclusivamente i privilegi di accesso ed utilizzo delle risorse gestite tramite il database management system strettamente necessari per l'espletamento delle attività di propria competenza.

5. Per ciascun applicativo è definito almeno un gruppo per ciascuna delle diverse tipologie di utenza previste da ogni specifico applicativo.
6. La definizione di gruppi aggiuntivi può essere decisa dal capo dell'ufficio.

Articolo 9
Monitoraggio del sistema.

1. Tutte le attività relative all'utilizzo e alla gestione del sistema informativo sono sottoposte ad un processo continuo di controllo e verifica della loro corretta e completa esecuzione. Tale processo trova attuazione innanzitutto attraverso l'utilizzo di appositi strumenti di controllo a livello di sistema, di database management system e di applicativo.
2. Il sistema consente le seguenti misure minime di monitoraggio a garanzia dell'autenticità e integrità dei dati:
a) la registrazione di tutti i tentativi di accesso effettuati, riusciti o falliti, a livello di sistema, di database management system e di applicativo;
b) gli accessi in lettura e scrittura effettuati direttamente attraverso il database management system;
c) tutti gli accessi in lettura e scrittura.
3. È cura dell'amministratore di sistema controllare periodicamente le registrazioni di cui al comma 3, lettere a) e b), allo scopo di rilevare eventuali anomalie e conservare le registrazioni dei log provvedendo alla trascrizione settimanale su supporti non riscrivibili da conservare unitamente ai backup dei registri.

Articolo 10
Disponibilità dei dati.

1. Presso ciascun ufficio sono previste idonee politiche e procedure per il salvataggio (backup) e per il recupero (recovery) dei dati, sia a livello di sistema, sia a livello di database management system.
2. Nell'àmbito delle politiche di cui al comma 1 è prevista la frequenza del salvataggio dei dati che non può essere superiore alla settimana.
3. Le procedure di backup consentono di conservare i dati per il tempo previsto dal decreto del Presidente della Repubblica 30 settembre 1963, n. 1409 e mediante l'utilizzo di supporti non riscrivibili, rinnovati a scadenze prestabilite e secondo le regole tecniche emanate dall'autorità per l'informatica nella pubblica amministrazione (2) a norma dell'art. 6, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
4. Le procedure di backup consentono di effettuare, con frequenza almeno triennale, una copia storica dei dati, che dovrà essere conservata secondo le modalità di cui al comma 3. Eseguita tale operazione, dal registro in uso possono essere eliminati i dati relativi agli affari esauriti da almeno due anni.
(2) La denominazione «Autorità per l'informatica nella pubblica amministrazione» è da intendersi sostituita da quella di «Centro nazionale per l'informatica nella pubblica amministrazione» ai sensi di quanto disposto dall'art. 176, D.Lgs. 30 giugno 2003, n. 196.

Capo III - Misure di tipo fisico e logico

Articolo 11
Infrastruttura logistica.

1. Le macchine server sono collocate in un apposito locale (sala server), dotato di impianto elettrico ed impianto di condizionamento opportunamente dimensionati e adeguatamente protetto dai rischi di incendio e allagamento.
2. L'accesso alla sala server è consentito sotto la responsabilità dell'amministratore di sistema.
3. Tutti i server sono asserviti a gruppi di continuità.
4. I supporti di backup sono custoditi in armadi blindati e ignifughi, posti in locali diversi dalla sala server.

Articolo 12
Software.

1. Presso l'ufficio è possibile installare ed utilizzare esclusivamente software appartenente ad una delle tre seguenti categorie:
a) software commerciale;
b) applicativi di rilevanza nazionale;
c) applicativi realizzati a livello locale.
2. L'installazione di software diverso da quello indicato alle lettere a) e b) del comma 1 è autorizzata dal capo dell'ufficio nel rispetto di quanto previsto dall'art. 18, commi 4 e 5.
3. È possibile installare ed utilizzare software commerciale solo se munito di idonea licenza d'uso, ovvero se fornito, nell'àmbito di accordi-quadro a livello nazionale, dall'URSIA.
4. Relativamente agli applicativi realizzati a livello locale è possibile installare ed utilizzare solo quelli dei quali sia stata verificata la conformità secondo le procedure di cui all'art. 18.
5. Il software è installato solo ed esclusivamente a partire da supporti fisici originali, ovvero da supporti fisici per i quali sia nota e sicura la provenienza.

Articolo 13
Dati.

1. Gli archivi informatici sono gestiti tramite software per la gestione di basi di dati (database management system).
2. Il piano per la sicurezza indica una strategia di adeguamento degli eventuali software diversi da quello indicato al comma 1.
3. L'accesso ai dati degli archivi informatici avviene solo ed esclusivamente per il tramite degli applicativi appartenenti al sottosistema applicativo, fatta eccezione per gli amministratori delle basi di dati relative all'archivio stesso, per i quali vale quanto prescritto dal comma 4.
4. L'accesso ai dati degli archivi informatici, da parte degli amministratori di basi di dati, avviene solo ed esclusivamente per il tramite degli strumenti messi a disposizione dal relativo database management system. Tutte le operazioni effettuate, da parte degli amministratori delle basi di dati sono soggette a registrazione, secondo quanto previsto all'art. 9, comma 1, lettera a). Le registrazioni di tali operazioni sono salvate su supporto fisico contestualmente alle ordinarie operazioni di backup e conservate per un periodo non inferiore a due anni.

Articolo 14
Gestione delle utenze.

1. L'amministratore di sistema e i suoi collaboratori, ciascuno per quanto di competenza, effettuano le seguenti operazioni:
a) creazione delle utenze e dei gruppi, secondo quanto previsto agli articoli 8 e 19;
b) assegnazione di nome utente e parola chiave a ciascun utente;
c) mantenimento di un elenco completo dei gruppi e delle utenze. Per ciascun gruppo sono indicati almeno l'identificativo, la data di creazione, la lista dei privilegi e l'eventuale data di disabilitazione; per ciascun gruppo sono indicati almeno il nome e il cognome, i gruppi di appartenenza, la data di creazione e la data di disabilitazione.
2. Le utenze non possono essere cancellate, ma solo disabilitate.
3. Le politiche per l'aggiornamento delle parole chiave sono definite nel piano per la sicurezza.

Articolo 15
Backup e recovery.

1. Nel piano per la sicurezza vengono individuati i dati da sottoporre a backup, nonché le modalità e la frequenza della procedura.
2. I dati oggetto di backup sono classificati in dati di sistema (necessari per il corretto funzionamento del sistema operativo, del software di base, del database management system, delle applicazioni installate, ecc.) e dati utente (documenti, fogli elettronici, archivi di posta elettronica, ecc.).
3. L'amministratore di sistema mette a disposizione di ciascun utente un'opportuna quota di spazio su disco disponibile per il backup dei dati utente. L'accesso a ciascuna quota è tale da consentire l'accesso in lettura e scrittura solo ed esclusivamente all'utente proprietario e l'accesso in sola lettura all'amministratore di sistema. È cura di ciascun utente provvedere a copiare sulla propria quota di spazio i file che desidera sottoporre a backup.

4. L'amministratore di sistema, secondo quanto indicato nel piano per la sicurezza:
a) garantisce l'effettiva messa in opera delle procedure di backup;
b) verifica l'avvenuta esecuzione dei backup;
c) mantiene un elenco delle operazioni di backup effettuate;
d) archivia i supporti fisici;
e) effettua, in caso di mal funzionamento, le procedure di recovery;
f) effettua verifiche periodiche delle procedure di recovery, secondo quanto disposto dal piano per la sicurezza;
g) mantiene un elenco dei problemi verificatisi e delle operazioni di recovery effettuate.

Articolo 16
Archiviazione ottica.

1. Il sistema informatico è dotato di almeno un sistema per la scrittura di supporti ottici, le cui caratteristiche siano conformi alle regole tecniche emanate dall'autorità per l'informatica nella pubblica amministrazione (3) a norma dell'art. 6, comma 2, del decreto del Presidente della Repubblica n. 445, del 2000.
2. Le applicazioni consentono l'archiviazione dei documenti in almeno uno dei formati indicati nelle regole tecniche di cui al comma 1.
3. Il sistema di archiviazione consente la generazione dei file di controllo e di chiusura, secondo le regole tecniche di cui al comma 1.
4. L'amministratore di sistema ottempera agli obblighi stabiliti dalle regole tecniche di cui al comma 1.
() La denominazione «Autorità per l'informatica nella pubblica amministrazione» è da intendersi sostituita da quella di «Centro nazionale per l'informatica nella pubblica amministrazione» ai sensi di quanto disposto dall'art. 176, D.Lgs. 30 giugno 2003, n. 196.

Articolo 17
Antivirus.

1. L'URSIA provvede alla distribuzione periodica a tutti gli uffici di un software antivirus e al suo costante aggiornamento.
2. Il piano per la sicurezza stabilisce le modalità di aggiornamento del software antivirus sulle postazioni di lavoro.

Capo IV - Misure relative agli applicativi

Articolo 18
Utilizzo degli applicativi.

1. Per la gestione informatizzata dei registri è possibile utilizzare applicativi di rilevanza nazionale o applicativi realizzati a livello locale.
2. Gli applicativi di rilevanza nazionale sono rilasciati dall'URSIA, che ne certifica la conformità ai sensi dell'art. 3 del decreto 27 marzo 2000, n. 264, del Ministro della giustizia.
3. Nessuna modifica o personalizzazione di applicativi di rilevanza nazionale è consentita da parte di soggetti diversi dall'URSIA.
4. Gli applicativi realizzati nell'àmbito di iniziative locali sono conformi alle regole tecniche ed alle presenti regole procedurali.
5. La conformità dei programmi alle caratteristiche previste nel presente capo viene certificata dall'URSIA.

Articolo 19
Caratteristiche degli applicativi.

1. Gli applicativi di cui all'art. 12, comma 1, lettere b) e c), sono sviluppati da società dotate di certificato di qualità EN ISO 9001, relativo ai servizi di sviluppo di prodotti software (CPV 7720-7721-7723).

2. Gli applicativi che gestiscono i registri consentono l'estrazione e la stampa dei dati, ai sensi dell'art. 6, comma 3, del decreto 27 marzo 2000, n. 264, del Ministro della giustizia.

3. L'applicativo consente, come misura minima relativa all'autenticazione degli utenti, l'accesso ai dati con un meccanismo di autenticazione basato sulla conoscenza di una coppia (username, password).
4. L'autenticazione di cui al comma 3 è effettuata tramite un meccanismo a sfida che non richieda il transito della password sulla rete.
5. L'autenticazione può essere effettuata una sola volta al momento dell'accesso al sistema informatico, oppure essere ripetuta al momento dell'accesso a ciascun programma.
6. L'applicativo fornisce un meccanismo di gestione degli accessi che consente di applicare quanto disposto dagli articoli 8 e 14.
7. L'accesso agli archivi informatici da parte degli utenti è consentito solo ed esclusivamente tramite le componenti del sottosistema applicativo.
8. L'accesso alle basi di dati da parte degli amministratori di basi di dati è consentito solo ed esclusivamente tramite l'utilizzo degli opportuni strumenti software di amministrazione.
9. Il piano per la sicurezza indica una strategia di adeguamento degli applicativi che non soddisfino i requisiti di cui ai precedenti commi.

Articolo 20
Documentazione.

1. L'applicativo è accompagnato da apposita documentazione di utilizzo, costituita da un manuale di amministrazione ed un manuale di utilizzo, e disponibile sia in forma cartacea che in forma elettronica.
2. La documentazione elettronica soddisfa i seguenti requisiti:
a) essere consultabile con modalità del tutto compatibili con quelle disponibili nel sistema operativo utilizzato;
b) consentire una navigazione ipertestuale rispetto a termini e argomenti chiave;
c) permettere di effettuare ricerche per sommario, indice e testo libero;
d) rendere disponibile una modalità di consultazione dipendente dal contesto, in modo tale da attivare le pagine relative all'argomento corrispondente alla funzionalità correntemente utilizzata.
3. Il manuale di amministrazione contiene almeno le seguenti informazioni:
a) requisiti hardware e software;
b) procedura di installazione;
c) gestione dei gruppi e degli utenti;
d) procedure operative;
e) procedure di aggiornamento;
f) procedure di backup e recovery;
g) gestione dei mal funzionamenti.
4. Il manuale di utilizzo contiene almeno le seguenti informazioni:
a) descrizione generale dell'applicativo;
b) descrizione della procedura di accesso e di uscita dall'applicativo;
c) modalità di utilizzo;
d) elenco di tutte le funzionalità;
e) elenco dei possibili messaggi di errore e guida alla risoluzione dei problemi;
f) glossario dei termini.
5. Per ciascuna funzionalità di cui al comma 4, lettera d), il manuale di utilizzo contiene le seguenti informazioni:
a) finalità della funzione;
b) modalità di accesso;
c) prerequisiti per l'utilizzo;
d) descrizione delle maschere che compaiono sul video;
e) dati richiesti dall'applicativo per l'esecuzione.
6. L'applicativo è corredato dal codice sorgente e da tutta la documentazione tecnica, sia in formato elettronico che cartaceo, prodotta durante l'intero ciclo di vita del software, coerentemente con le norme di qualità di cui all'art. 19, comma 1.

Articolo 21
Servizi accessori.

1. L'applicativo è corredato da idoneo servizio di manutenzione correttiva ed evolutiva, nonché da idoneo servizio di assistenza tecnica.

Capo V - Comportamento dell'utente

Articolo 22
Manuale per l'utente.

1. L'utente del sistema informativo dell'ufficio è tenuto ad osservare comportamenti atti a ridurre al minimo i rischi di perdita, danneggiamento o diffusione non autorizzata dei dati a garanzia della integrità e autenticità degli stessi.
2. I comportamenti di cui al comma 1 sono descritti negli articoli 23, 24, 25 mentre i comportamenti di maggior dettaglio sono riportati in un apposito manuale per l'utente, da stilare, a cura dell'amministratore di sistema, sulla base delle presenti regole procedurali e del piano per la sicurezza.

Articolo 23
Regole di tipo fisico.

1. L'utente è tenuto, ove sia possibile, a chiudere a chiave la porta del proprio ufficio e a tenere sotto chiave i propri documenti, indipendentemente dal supporto fisico utilizzato.
2. L'utente è tenuto, allontanandosi momentaneamente dalla postazione di lavoro, a chiudere le applicazioni attive o a proteggerla tramite password del salvaschermo.
3. L'utente è tenuto, al termine della giornata di lavoro, a spegnere la postazione.
4. L'utente è tenuto ad assicurarsi dell'identità e delle autorizzazioni di personale che debba installare il nuovo software o hardware sulla propria postazione di lavoro.
5. L'utente è tenuto a non utilizzare, su postazioni di lavoro collegate alla rete locale dell'ufficio, modem o altri strumenti di connessione con l'esterno.

Articolo 24
Regole di tipo logico.

1. L'utente è tenuto a non installare sulla propria postazione di lavoro alcun programma non preventivamente autorizzato dal capo dell'ufficio.
2. L'utente può, qualora lo reputi necessario, configurare o richiedere la configurazione della propria postazione di lavoro in modo che venga richiesta una password all'accensione.
3. Il capo dell'ufficio può assegnare all'utente un programma per la cifratura dei dati sul disco rigido, su motivata richiesta scritta di quest'ultimo o per espresse esigenze di ufficio.
4. L'amministratore di sistema, su incarico del responsabile della tenuta dei registri, stabilisce le procedure di utilizzo dei programmi di cui al comma 3.
5. L'utente che utilizzi, per le proprie necessità di lavoro, un computer portatile:
a) risponde personalmente dei dati sul portatile in dotazione;
b) è motivato a effettuare la richiesta di cui al comma 3;
c) può richiedere all'amministratore di sistema l'assegnazione di una quota disco, di cui all'art. 15, comma 3, per il backup dei dati del portatile.
6. L'utente è tenuto a non diffondere messaggi di posta elettronica di provenienza dubbia ed a non partecipare alle cosiddette «catene di S. Antonio» o simili.

Articolo 25
Gestione delle password.

1. L'utente è tenuto:
a) a non rivelare a terzi la propria password;
b) a non scrivere la password in punti facilmente visibili;
c) a digitare la password al riparo da sguardi indiscreti.
2. L'utente sceglie la propria password:
a) diversa dal proprio username;
b) non costituita da una semplice parola rintracciabile in un dizionario;
c) non legata alla propria vita personale;

d) con una lunghezza non inferiore a sei caratteri;

e) contenente almeno un simbolo diverso da una lettera, oppure un misto di lettere maiuscole e minuscole.
3. La password è cambiata con frequenza almeno annuale.
4. L'amministratore di sistema ha facoltà di stabilire una frequenza di cambio della password superiore a quanto stabilito nel comma 3, nonché di configurare il sistema e gli applicativi in modo da forzare l'utente al cambio allo scadere del termine fissato.

Capo VI - Disposizioni finali

Articolo 26
Tempi di attuazione.

1. I tempi di attuazione delle presenti regole procedurali sono i seguenti, con decorrenza dalla data della loro pubblicazione:
a) entro sei mesi è preparato il piano di adeguamento degli applicativi di cui all'art. 19, comma 9;
b) entro dodici mesi è completata la prima versione del piano per la sicurezza di cui all'art. 7;
c) entro diciotto mesi sono adottate presso l'ufficio tutte le prescrizioni relative all'infrastruttura tecnologica di cui al capo III e all'infrastruttura logistica di cui al capo IV;
d) entro tre anni, tutti gli applicativi in uso sono adeguati alle prescrizioni del capo IV e dell'art. 16.

D.M. 27 marzo 2000, n. 264
Regolamento recante norme per la tenuta dei registri presso gli uffici giudiziari

Capo I - Princìpi generali

1. Definizioni.

1. Agli effetti del presente regolamento, si intende per:
a) «registri»: i registri tenuti, a cura delle cancellerie o delle segreterie, presso gli uffici giudiziari, ovvero i registri previsti da codici, da leggi speciali o da regolamenti, comunque connessi all'espletamento delle attribuzioni e dei servizi svolti dall'Amministrazione della giustizia;
b) «atti»: gli atti formati o comunicati dalle cancellerie o segreterie degli uffici giudiziari;
c) «tenuta dei registri»: la formazione, l'uso, la conservazione, la custodia, l'esibizione di registri;
d) «regole tecniche»: le regole emanate dall'Autorità per l'informatica nella pubblica amministrazione ai sensi del decreto Presidente della Repubblica 10 novembre 1997, n. 513;
e) «codice di identificazione»: il codice idoneo ad assicurare l'identificazione della persona che accede ai registri;
f) «regole procedurali»: le regole emanate, in ossequio alle esigenze relative alla integrità fisica e logica dei dati, con decreto del Ministro della giustizia sulla tipologia dei dati stessi da inserire negli atti e nei registri anche ai sensi del decreto del Presidente della Repubblica 28 ottobre 1994, n. 748;
g) «responsabile dei sistemi informativi automatizzati»: il dirigente generale o equiparato di cui all'articolo 10 del decreto legislativo 12 febbraio 1993, n. 39.

2. Princìpi generali sulla tenuta dei registri.

1. I registri sono tenuti su base annuale ed in modo da garantire la integrità, la completezza, la disponibilità e la riservatezza di iscrizioni ed annotazioni nonché la identificazione del soggetto che accede ai registri.

3. Tenuta dei registri.

1. I registri sono tenuti in modo informatizzato secondo le regole procedurali.

2. La conformità alle regole tecniche e alle regole procedurali è certificata dal responsabile dei sistemi informativi automatizzati, di cui all'articolo 10 del decreto legislativo 12 febbraio 1993, n. 39, del Ministro della giustizia prima della messa in uso del sistema.
3. La competente articolazione del Ministero della giustizia o del diverso Ministero presso cui i registri di cui all'articolo 13 sono istituiti può, su richiesta motivata del capo dell'ufficio interessato e sentito il responsabile dei sistemi informativi automatizzati, autorizzarne la tenuta su supporto cartaceo.

4. Modalità di tenuta dei registri.

1. La tenuta informatizzata dei registri secondo le regole tecniche e le regole procedurali di attuazione garantisce la integrità, la disponibilità e la riservatezza dei dati e consente l'identificazione del soggetto che accede al registro;
2. I registri tenuti su supporto cartaceo, prima di essere posti in uso, sono numerati e vidimati in ogni mezzo foglio dal dirigente della cancelleria o della segreteria dell'ufficio o da persona da lui delegata.

5. Rilascio di informazioni, copie, estratti e certificati.

1. L'accesso alle informazioni contenute nei registri e il rilascio di copie, estratti o certificati è disciplinato secondo i seguenti livelli:
a) pubblico;
b) limitato agli aventi diritto;
c) consentito solo previa autorizzazione dell'autorità competente secondo la legge;
d) riservato agli uffici e alle autorità specificamente individuati dalla legge.
2. Nel sistema informatico a ciascun livello di accesso viene attribuito uno specifico codice di identificazione.

Capo II - Dei registri informatizzati

6. Tenuta informatizzata dei registri.

1. I registri informatizzati contengono i dati e l'aggregazione dei dati di cui ai modelli dei registri previsti dall'articolo 13 del presente regolamento, e comunque da ogni altra disposizione di legge.
2. I dati di cui al comma 1 possono essere contenuti in uno o più supporti informatici. Il sistema consente la possibilità di estrazione dei dati secondo la natura delle controversie, la sezione, il giudice, il nome delle parti, lo stato della causa, la udienza ed ogni altro tipo di dato eventualmente richiesto dalle disposizioni che regolano la tenuta dei registri e la loro individuazione.
3. I registri informatizzati consentono la loro riproduzione, per intero o per estratto, anche su supporto cartaceo.

7. Soggetti.

1. Il dirigente amministrativo dell'ufficio indica per iscritto le persone autorizzate alle operazioni di immissione, cancellazione, variazione ed esibizione.
2. La identificazione di colui che effettua le operazioni di cui al comma 1, con l'indicazione della relativa data ed ora, è conservata nel sistema informatico.

8. Interruzione del funzionamento.

1. In caso di interruzione del funzionamento del sistema informatico l'ufficio provvede alla ricezione degli atti apponendo su ciascuno di essi la data, l'ora, se richiesta dalla legge o dalla natura dell'atto, e un numero progressivo provvisorio. Gli atti vengono, successivamente inseriti nel sistema informatico secondo l'ordine risultante dalla data e dal numero provvisorio.
2. Se gli uffici preposti alla ricezione degli atti sono in numero superiore ad uno, l'ordine di inserimento degli atti depositati è indicato dalla data di deposito, dal numero progressivo che contrassegna il terminale esistente presso l'ufficio che ha ricevuto l'atto e dal numero provvisorio.

9. Informatizzazione degli atti.

1. Gli atti sono formati mediante sistemi informatici conformi alle disposizioni di cui al decreto legislativo 12 febbraio 1993, n. 39.
2. Se la legge richiede la sottoscrizione dell'atto a pena di nullità, l'autenticità ne è attestata mediante la firma digitale, secondo le regole tecniche.
3. L'indicazione a stampa, sui documenti o certificati estratti dal sistema informatico, del nominativo del firmatario è equipollente, per la validità dell'atto, all'apposizione di firma autografa.
4. Il sistema informatico consente di effettuare riproduzioni, copie o estratti, anche su supporto cartaceo.

10. Comunicazione dei dati contenuti nei registri e degli atti.

1. Il sistema informatico è strutturato con modalità che assicurano:
a) l'individuazione dell'ufficio al quale il registro appartiene;
b) l'individuazione del soggetto che inserisce, modifica o comunica il dato;
c) l'avvenuta ricezione della comunicazione del dato.

11. Modalità di accesso ai registri e agli atti.

1. L'accesso ai registri e agli atti informatizzati è effettuato dall'interessato direttamente o tramite l'ufficio depositario ovvero per via telematica, previa identificazione del medesimo secondo le regole procedurali.
2. In caso di rilascio di riproduzioni, copie, estratti o certificati per via telematica, la conformità di quanto trasmesso all'originale è attestata nelle forme previste dalla legge in relazione alla natura dell'atto.
3. Quando è previsto il pagamento di diritti, imposte o tasse, il rilascio di riproduzioni, copie, estratti o certificati per via telematica è subordinato al previo pagamento degli stessi, della cui avvenuta riscossione è dato atto nella copia, estratto o certificato trasmessi.

12. Obblighi di conservazione e di custodia.

1. I registri e gli atti tenuti in modo informatico sono conservati per il tempo previsto dal decreto legislativo 29 ottobre 1999, n. 490.
2. I soggetti di cui all'articolo 7, comma 1, curano la conservazione dei registri e degli atti di cui al precedente comma 1, mediante l'utilizzo di supporti non riscrivibili, rinnovati a scadenze prestabilite e secondo le regole tecniche emanate dall'Autorità per l'informatica nella pubblica amministrazione a norma dell'articolo 2, comma 15, della legge 24 dicembre 1993, n. 537.
3. I soggetti di cui al comma 2 procedono, almeno ogni tre anni, alla formazione di una copia storica dell'archivio e ne dispongono la conservazione nei modi di cui al comma 2. Eseguita tale operazione dal registro in uso possono essere eliminati gli atti relativi agli affari esauriti da almeno due anni.

Capo III - Individuazione dei registri

13. Elenco dei registri.

1. Presso il tribunale sono tenuti i seguenti registri:
1) ruolo generale degli affari civili - cause ordinarie;
2) ruolo generale degli affari civili - procedimenti speciali sommari;

3) ruolo generale degli affari civili - controversie in materia di lavoro e di previdenza e di assistenza obbligatorie;

4) ruolo generale degli affari civili - controversie agrarie;
5) ruolo sezionale per le cause ordinarie;
6) ruolo delle cause assegnate a ciascun giudice;
7) ruolo delle controversie in materia di lavoro e di previdenza e di assistenza obbligatoria assegnate a ciascun giudice;
8) ruolo delle udienze per ciascun giudice istruttore;
9) ruolo delle udienze in materia lavoro e di previdenza o assistenza obbligatoria;
10) registro dei provvedimenti di cui agli articoli 186-bis, 186-ter, 186-quater del codice di procedura civile;
11) registro dei provvedimenti cautelari e d'urgenza;
12) registro del deposito delle ordinanze pronunziate fuori udienza;
13) ruolo dei reclami avverso i provvedimenti cautelari e d'urgenza;
14) ruolo delle udienze collegiali;
15) ruolo delle udienze collegiali per le controversie agrarie;
16) registro delle sentenze e degli altri provvedimenti emessi e pubblicati;
17) registro degli affari amministrativi e stragiudiziali;
18) ruolo generale degli affari civili non contenziosi e da trattarsi in camera di consiglio;
19) ruolo generale delle esecuzioni civili;
20) ruolo generale delle espropriazioni immobiliari;
21) registro degli incarichi conferiti e dei compensi liquidati ai notai per le operazioni di vendita;
22) ruolo delle istanze per la dichiarazione di fallimento;
23) registro dei fallimenti dichiarati;
24) pubblico registro dei falliti;
25) registro dei concordati preventivi;
26) registro delle amministrazioni concordate;
27) registro delle liquidazioni coatte amministrative;
28) registro delle amministrazioni straordinarie;
29) [registro per l'annotazione delle spese anticipate dall'erario nelle procedure fallimentari] (2/b);
30) registro delle adozioni;
31) registro degli interdetti e degli inabilitati;
32) registro delle tutele dei minori e degli interdetti;
33) registro delle curatele dei minori emancipati e degli inabilitati;
34) registro delle istanze al giudice tutelare;
35) registro delle successioni;
36) registro delle persone giuridiche;
37) registro per la trascrizione delle vendite con patto di riservato dominio;
38) registro degli incarichi affidati e dei compensi liquidati ai consulenti tecnici, ai legali e ai curatori, commissari e liquidatori fallimentari;
39) [registro per le istanze di ammissione al gratuito patrocinio] (2/c);
40) [registro dei verbali di adunanza della commissione per il gratuito patrocinio] (2/d);
41) [registro delle spese di giustizia anticipate dall'erario] (2/e);
42) [registro delle spese concernenti le cause in cui siano parti persone o enti ammessi alla prenotazione a debito] (2/f);
43) registro per la pubblicazione di giornali e periodici;
44) registro cronologico dei provvedimenti e degli altri atti originali;
45) registro repertorio degli atti soggetti a registrazione;
46) registro per la trascrizione dei contratti e degli atti costitutivi di privilegi relativi a vendita o locazione di macchine utensili o di produzione di valore non inferiore a L. 1.000.000;
47) registro generale dei testamenti;
48) [registro dei ruoli] (2/g).
2. I registri di cui al comma 1, ad eccezione di quelli contraddistinti dai numeri 8, 9, 12, 14, 15, 16, 24, 34, 37, 44, 45, e 46, ove tenuti su supporto cartaceo, sono corredati da rubrica alfabetica (2/h).
3. Gli uffici giudiziari sottoindicati tengono i registri come di seguito precisato. Presso le sezioni staccate dei tribunali sono tenuti i medesimi registri previsti dai numeri 1, 2, 6, 8, 10, 11, 12, 16, 17, 18, 19, 20, 21, 32, 33, 34, 35, 38, 44, 45 del comma 1 (2/i).

4. Presso la corte di appello sono tenuti i registri previsti dai numeri 1, 3, 4, 5, 6, 8, 11, 12, 13, 14, 15, 16, 18, 38, 44, 45 del comma 1 (2/l).

5. Presso la Suprema corte di cassazione sono tenuti i seguenti registri:

1) ruolo generale degli affari civili e relativa rubrica alfabetica;
2) ruolo di udienza per ciascuna sezione;
3) registro cronologico dei provvedimenti e degli atti originali;
4) registro repertorio degli atti soggetti a registrazione;
5) [registro delle spese inerenti alle cause riflettenti persone o enti giuridici ammessi alla prenotazione a debito] (2/m).

6. Presso il giudice di pace sono tenuti i seguenti registri:
1) ruolo generale degli affari contenziosi civili e relativa rubrica alfabetica;
2) registro dei provvedimenti ex art. 186-bis, 186-ter, 186-quater;
3) registro del deposito delle ordinanze pronunziate fuori udienza;
4) registro delle sentenze e degli altri provvedimenti emessi e pubblicati;
5) ruolo di udienza;
6) ruolo generale degli affari amministrativi, stragiudiziali e non contenziosi e relativa rubrica alfabetica;
7) registro cronologico dei provvedimenti e degli altri atti originali;
8) registro repertorio degli atti soggetti a registrazione;
9) [registro delle spese di giustizia anticipate dall'erario] (2/n);
10) [registro delle spese concernenti le cause in cui siano parti persone o enti ammessi alla prenotazione a debito] (2/o);
11) registro degli incarichi conferiti e dei compensi liquidati ai consulenti tecnici;
12) [registro dei ruoli] (2/p).

(2/b) Numero abrogato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/c) Numero abrogato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/d) Numero abrogato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/e) Numero abrogato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/f) Numero abrogato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/g) Numero abrogato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/h) Comma così modificato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/i) Comma così modificato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/l) Comma così modificato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/m) Numero abrogato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/n) Numero abrogato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/o) Numero abrogato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.
(2/p) Numero abrogato dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 114 e dall'art. 301, comma 1, D.P.R. 30 maggio 2002, n. 115, con la decorrenza indicata nell'art. 302 dello stesso decreto.

14. Determinazione dei modelli dei registri.

1. Ciascuno dei registri indicati all'articolo 13 può consistere di uno o più modelli.
2. Con decreti del Ministro della giustizia, di concerto con il Ministro del tesoro, del bilancio e della programmazione economica, nei casi previsti dall'articolo 646 del regolamento per l'amministrazione del

patrimonio e per la contabilità generale dello Stato, approvato con regio decreto 23 maggio 1924, n. 827, sono stabiliti i modelli di cui al comma 1. Rimane fermo quanto previsto dall'articolo 33 del regio decreto 18 dicembre 1941, n. 1368 e dall'articolo 3 della legge 23 marzo 1956, n. 182.

Capo IV - Della raccolta dei provvedimenti

15. Archivio digitale dei provvedimenti.

1. Presso la cancelleria del tribunale e della corte di appello è istituito un archivio, tenuto ai sensi dell'articolo 12, comma 2, dove sono conservati, in copia, le sentenze e gli altri provvedimenti in materia civile e penale, che sono determinati con decreti del Ministro della giustizia.
2. I soggetti di cui all'articolo 7, comma 1, possono rilasciare copia autentica degli atti contenuti nell'archivio previsto dal comma 1 del presente articolo.

16. Prima copia dei provvedimenti in forma digitale.

1. I soggetti di cui all'articolo 7, comma 1, procedono:
a) al momento del deposito, a fare la copia digitale, da conservare nell'archivio di cui all'articolo 15, comma 1;
b) ad acquisire nell'archivio digitale ogni annotazione riportata sull'originale del provvedimento;
c) ad autenticare la copia informatica del provvedimento e le successive annotazioni mediante la firma digitale.

17. Archivio digitale dei provvedimenti del giudice di pace.

1. Presso la cancelleria del giudice di pace è istituito un archivio, tenuto ai sensi dell'articolo 12, comma 2, dove sono conservati, in copia, le sentenze, comprese quelle emesse ai sensi dell'articolo 281-sexies del codice di procedura civile, e gli altri provvedimenti di cui all'articolo 15, comma 1, se soggetti all'obbligo di registrazione.
2. Ferme le competenze dell'ufficio di cancelleria del giudice di pace in ordine agli adempimenti previsti dagli articoli 16 e 18, il supporto informatico contenente la raccolta dei provvedimenti, se sussistono ragioni organizzative e tecniche, può essere collocato presso il tribunale nel cui circondario si trova l'ufficio.
3. La decisione di collocare il supporto informatico fuori dell'ufficio del giudice di pace è assunta dalla competente articolazione del Ministero della giustizia sentiti il responsabile dei sistemi informativi automatizzati, il presidente del tribunale e il coordinatore dell'ufficio del giudice di pace.

18. Raccolta dei provvedimenti.

1. I soggetti di cui all'articolo 7, comma 1, procedono, almeno ogni tre anni, alla formazione di una copia dell'archivio mediante l'utilizzo di supporti non riscrivibili, secondo le regole tecniche emanate dall'Autorità per l'informatica nella pubblica amministrazione a norma dell'articolo 2, comma 15, della legge 24 dicembre 1993, n. 537. Eseguita tale operazione dalla raccolta di cui all'articolo 15, comma 1, possono essere eliminati i provvedimenti depositati da almeno tre anni.

Capo V - Norme finali e transitorie

19. Raccolta dei provvedimenti in originale.
1. Sono fatte salve le norme di cui agli articoli 35 del regio decreto 18 dicembre 1941, n. 1368, 16, comma 2 e 23 del decreto ministeriale 30 settembre 1989, n. 334, regolanti la raccolta annuale degli originali dei provvedimenti giurisdizionali.

20. Regole procedurali.

1. Entro tre mesi dalla pubblicazione del presente regolamento sono emanate le regole procedurali.

2. Nelle more della emanazione delle regole procedurali i sistemi informatici in uso possono essere utilizzati se assicurano il controllo dell'accesso ai dati e la integrità fisica degli stessi secondo gli standard indicati dall'ufficio del responsabile dei sistemi informativi automatizzati.

Varato il regolamento sui processi telematici

NUMERO SCHEDA: 703

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: PROCESSO TELEMATICO

FONTE: GAZZETTA UFFICIALE

NUMERO: 89

DATA: 07/04/2001

NATURA ATTO: D.P.R.

DATA ATTO: 13/02/2001

NUM. ATTO: 123

SCHEDE COLLEGATE: 6339

Il d.p.r. n. 123 del 13 febbraio 2001 "Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei Conti" prevede che "*tutti gli atti e i provvedimenti del processo possono essere compiuti come documenti informatici sottoscritti con firma digitale come espressamente previsto dal presente regolamento*" (art. 4, comma 1).
Questo regolamento non incide sulle disposizioni sostanziali processuali (adempimenti, termini, contenuto di atti, produzioni ecc.), ma pone solamente norme strumentali sull'uso di strumenti informatici e telematici nel processo che si affiancheranno alle modalità ordinarie (su supporto "cartaceo").
La nuova disciplina sarà applicabile ai giudizi iscritti a ruolo dopo il primo gennaio 2002 (art. 19 del Regolamento).

Si allega il testo.

D.P.R. 13 febbraio 2001, n. 123
Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti.

1. Definizioni.
1. Agli effetti del presente regolamento si intende per:
a) «documento informatico»: la rappresentazione informatica del contenuto di atti, fatti o dati giuridicamente rilevanti ai sensi del *decreto del Presidente della Repubblica 10 novembre 1997, n. 513*;
b) «duplicato del documento informatico»: la riproduzione del documento informatico effettuata su un qualsiasi tipo di supporto elettronico facilmente trasportabile;

c) «documento probatorio»: l'atto avente efficacia probatoria ai sensi del codice civile e del codice di procedura civile;
d) «firma digitale»: il risultato della procedura informatica disciplinata dal *decreto del Presidente della Repubblica 10 novembre 1997, n. 513*;
e) «dominio giustizia»: l'insieme delle risorse *hardware* e *software*, mediante il quale l'amministrazione della giustizia tratta in via informatica e telematica qualsiasi tipo di attività, di dato, di servizio, di comunicazione e di procedura;
f) «sistema informatico civile»: è il sottoinsieme delle risorse del dominio giustizia mediante il quale l'amministrazione della giustizia tratta il processo civile;
g) «gestore del sistema di trasporto delle informazioni»: il gestore indicato dall'articolo 13, comma 2, del *decreto del Presidente della Repubblica 10 novembre 1997, n. 513*;
h) «indirizzo elettronico»: l'indirizzo di posta elettronica come definito dall'articolo 1, comma 1, lettera *l*), del *decreto del Presidente della Repubblica 10 novembre 1997, n. 513*;
i) «ricevuta di consegna»: il messaggio generato ed inviato automaticamente al mittente dal gestore del sistema di trasporto delle informazioni del destinatario nel momento in cui il messaggio inviato è reso disponibile al destinatario medesimo nella sua casella di posta elettronica;
j) «certificatore della firma digitale»: il soggetto previsto dagli articoli 8, 9 e 17 del *decreto del Presidente della Repubblica 10 novembre 1997, n. 513*.

2. *Campo di applicazione.*
1. È ammessa la formazione, la comunicazione e la notificazione di atti del processo civile mediante documenti informatici nei modi previsti dal presente regolamento.
2. L'attività di trasmissione, comunicazione o notificazione, dei documenti informatici è effettuata per via telematica attraverso il sistema informatico civile, fatto salvo quanto stabilito dall'articolo 6.
3. Si applicano le disposizioni del *decreto del Presidente della Repubblica 10 novembre 1997, n. 513*, ove non diversamente stabilito dal presente regolamento.

3. *Sistema informatico civile.*
1. Il sistema informatico civile è strutturato con modalità che assicurano:
a) l'individuazione dell'ufficio giudiziario e del procedimento;
b) l'individuazione del soggetto che inserisce, modifica o comunica l'atto;
c) l'avvenuta ricezione della comunicazione dell'atto;
d) l'automatica abilitazione del difensore e dell'ufficiale giudiziario.
2. Al sistema informatico civile possono accedere attivamente soltanto i difensori delle parti e gli ufficiali giudiziari per le attività rispettivamente consentite dal presente regolamento.
3. Con decreto del Ministro della giustizia, sentita l'Autorità per l'informatica nella pubblica amministrazione, sono stabilite le regole tecnico-operative per il funzionamento e la gestione del sistema informatico civile, nonché per l'accesso dei difensori delle parti e degli ufficiali giudiziari. Con il medesimo decreto sono stabilite le regole tecnico-operative relative alla conservazione e all'archiviazione dei documenti informatici, conformemente alle prescrizioni di cui all'articolo 2, comma 15, della *legge 24 dicembre 1993, n. 537*, e all'articolo 18 del *decreto del Presidente della Repubblica 10 novembre 1997, n. 513* (2).
(2) In attuazione di quanto disposto dal presente comma vedi il *D.M. 14 ottobre 2004.*

4. *Atti e provvedimenti.*
1. Tutti gli atti e i provvedimenti del processo possono essere compiuti come documenti informatici sottoscritti con firma digitale come espressamente previsto dal presente regolamento.
2. Se non è possibile procedere alla sottoscrizione nella forma di cui al comma 1, gli atti e i provvedimenti vengono redatti o stampati su supporto cartaceo, sottoscritti nei modi ordinari e allegati al fascicolo cartaceo. La copia informatica degli stessi è inserita nel fascicolo informatico con le modalità di cui agli articoli 12 e 13.
3. Ove dal presente regolamento non è espressamente prevista la sottoscrizione del documento informatico con la firma digitale, questa è sostituita dall'indicazione del nominativo del soggetto procedente prodotta sul documento dal sistema automatizzato, a norma dell'articolo 3, comma 2, del *decreto legislativo 12 febbraio 1993, n. 39*.

5. *Processo verbale.*
1. Il processo verbale, redatto come documento informatico, è sottoscritto con firma digitale da chi presiede l'udienza e dal cancelliere. Nei casi in cui è richiesto, le parti e i testimoni procedono alla sottoscrizione delle dichiarazioni o del verbale apponendo la propria firma digitale.

2. Se non è possibile procedere alla sottoscrizione nella forma di cui al comma 1, il processo verbale viene redatto o stampato su supporto cartaceo, sottoscritto nei modi ordinari e allegato al fascicolo cartaceo. La copia informatica del processo verbale è allegata al fascicolo informatico con le modalità di cui agli articoli 12 e 13.

6. Comunicazioni e notificazione.

1. Le comunicazioni con biglietto di cancelleria, nonché la notificazione degli atti, effettuata quest'ultima come documento informatico sottoscritto con firma digitale, possono essere eseguite per via telematica, oltre che attraverso il sistema informatico civile, anche all'indirizzo elettronico dichiarato ai sensi dell'articolo 7.
2. La parte che richiede la notificazione di un atto trasmette per via telematica l'atto medesimo all'ufficiale giudiziario, che procede alla notifica con le medesime modalità.
3. L'ufficiale giudiziario, se non procede alla notificazione per via telematica, trae dall'atto ricevuto come documento informatico la copia su supporto cartaceo, ne attesta la conformità all'originale e provvede a notificare la copia stessa unitamente al duplicato del documento informatico, nei modi di cui agli articoli 138 e seguenti del codice di procedura civile.
4. Eseguita la notificazione, l'ufficiale giudiziario restituisce per via telematica l'atto notificato, munito della relazione della notificazione attestata dalla sua firma digitale.

7. Indirizzo elettronico.

1. Ai fini delle comunicazioni e delle notificazioni ai sensi dell'articolo 6, l'indirizzo elettronico del difensore è unicamente quello comunicato dal medesimo al Consiglio dell'ordine e da questi reso disponibile ai sensi del comma 3 del presente articolo. Per gli esperti e gli ausiliari del giudice l'indirizzo elettronico è quello comunicato dai medesimi ai propri ordini professionali o all'albo dei consulenti presso il tribunale.
2. Per tutti i soggetti diversi da quelli indicati nel comma 1, l'indirizzo elettronico è quello dichiarato al certificatore della firma digitale al momento della richiesta di attivazione della procedura informatica di certificazione della firma digitale medesima, ove reso disponibile nel certificato.
3. Gli indirizzi elettronici di cui al comma 1, comunicati tempestivamente dagli ordini professionali al Ministero della giustizia, nonché quelli degli uffici giudiziari e degli uffici notifiche (UNEP), sono consultabili anche in via telematica secondo le modalità operative stabilite dal decreto di cui all'articolo 3, comma 3.

8. Attestazione temporale.

1. La comunicazione e la notificazione si ha per eseguita alla data apposta dal notificatore alla ricevuta di consegna mediante la procedura di validazione temporale a norma del *decreto del Presidente della Repubblica 10 novembre 1997, n. 513*. Per la comunicazione e la notificazione eseguite dalla cancelleria e dall'ufficiale giudiziario la data riportata nella ricevuta di consegna tiene luogo della suddetta procedura di validazione temporale.
2. I dati relativi a quanto previsto dal comma 1, sono conservati dal notificatore per un periodo non inferiore a cinque anni secondo le modalità tecnico-operative stabilite dal decreto di cui all'articolo 3, comma 3.

9. Costituzione in giudizio e deposito.

1. La parte che procede all'iscrizione a ruolo o alla costituzione in giudizio per via telematica trasmette con il medesimo mezzo i documenti probatori come documenti informatici o le copie informatiche dei documenti probatori su supporto cartaceo.

10. Procura alle liti.

1. Se la procura alle liti è stata conferita su supporto cartaceo, il difensore, che si costituisce per via telematica, trasmette la copia informatica della procura medesima, asseverata come conforme all'originale mediante sottoscrizione con firma digitale.

11. Iscrizione a ruolo.

1. La nota di iscrizione a ruolo può essere trasmessa per via telematica come documento informatico sottoscritto con firma digitale.
2. La nota di iscrizione a ruolo trasmessa per via telematica è redatta in modo conforme al modello definito con il decreto di cui all'articolo 3, comma 3.

12. Fascicolo informatico.

1. La cancelleria procede alla formazione informatica del fascicolo d'ufficio, contenente gli atti del processo come documenti informatici ovvero le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo.
2. Nel fascicolo informatico sono inseriti, secondo le modalità di cui al comma 1, anche i documenti probatori offerti in comunicazione o prodotti dalle parti o comunque acquisiti al processo. Per i

documenti probatori prodotti o comunque acquisiti su supporto cartaceo l'inserimento nel fascicolo informatico delle relative copie informatiche è effettuato dalla cancelleria, sempre che l'operazione non sia eccessivamente onerosa.
3. La formazione del fascicolo informatico non elimina l'obbligo di formazione del fascicolo d'ufficio su supporto cartaceo.

13. *Formazione del fascicolo informatico.*

1. Ogni fascicolo informatico riceve la stessa numerazione del fascicolo cartaceo ed è formato secondo quanto stabilito dall'articolo 36 delle norme di attuazione del codice di procedura civile.
2. L'indice degli atti contiene anche l'indicazione dei documenti conservati solo nel fascicolo cartaceo ed è redatto in modo da consentire la diretta consultazione degli atti e dei documenti informatici.
3. Gli atti e i documenti probatori depositati dalle parti, contestualmente alla costituzione in giudizio o successivamente, sono inseriti in apposite sezioni del fascicolo informatico contenenti ciascuna l'indicazione del giudizio e della parte cui si riferiscono.
4. Ai sensi dell'articolo 12, comma 2, è eccessivamente onerosa l'estrazione della copia informatica di documenti probatori prodotti o acquisiti su supporto cartaceo, ai fini dell'inserimento nel fascicolo informatico da parte della cancelleria, quando il formato del documento da copiare è diverso da quelli indicati con il decreto di cui all'articolo 3, comma 3, ovvero se il numero delle pagine da copiare è superiore a venti. Con il medesimo decreto il numero delle pagine è periodicamente aggiornato.
5. In deroga al comma 4 la cancelleria procede comunque all'estrazione della copia informatica di documenti probatori prodotti o acquisiti su supporto cartaceo quando la parte allega ad essi la copia su supporto informatico.
6. Il fascicolo informatico è consultabile dalla parte, oltre che in via telematica, anche nei locali della cancelleria attraverso un videoterminale.
7. Dopo la precisazione delle conclusioni il responsabile della cancelleria appone al fascicolo informatico la firma digitale.

14. *Produzione degli atti e dei documenti probatori su supporto informatico.*

1. Gli atti e i documenti probatori offerti in comunicazione dalle parti dopo la costituzione in giudizio possono essere prodotti, oltre che per via telematica, anche mediante deposito in cancelleria del supporto informatico che li contiene. Il supporto informatico deve essere compatibile con i tipi e i modelli stabiliti al riguardo dal decreto di cui all'articolo 3, comma 3, e deve contenere anche il relativo indice, la cui integrità è attestata dal difensore con la firma digitale.
2. Il responsabile della cancelleria procede a duplicare nel fascicolo informatico gli atti, i documenti probatori e l'indice indicati nel comma 1.
3. Il supporto informatico è restituito alla parte dopo la duplicazione di cui al comma 2.

15. *Deposito della relazione del C.T.U.*

1. La relazione prevista dall'articolo 195 del codice di procedura civile può essere depositata per via telematica come documento informatico sottoscritto con firma digitale.
2. Con lo stesso mezzo devono essere allegati i documenti e le osservazioni delle parti o la copia informatica di questi ove gli originali sono stati prodotti su supporto cartaceo. In tal caso gli originali sono depositati dal consulente tecnico d'ufficio senza ritardo, in ogni caso prima dell'udienza successiva alla scadenza del termine per il deposito della relazione.
3. Il giudice, tenuto conto di un eventuale successivo utilizzo dei dati contenuti nella consulenza tecnica d'ufficio, può disporre che la relazione o parte di essa sia redatta in modo conforme a modelli definiti con il decreto di cui all'articolo 3, comma 3.

16. *Trasmissione dei fascicoli.*

1. Qualora non sia necessario acquisire il fascicolo d'ufficio su supporto cartaceo, la trasmissione del fascicolo d'ufficio può avvenire, in ogni stato e grado, anche per via telematica con particolari modalità, stabilite con il decreto di cui all'articolo 3, comma 3, e dirette ad assicurarne l'integrità, l'autenticità e la riservatezza.
2. Prima dell'inoltro, il responsabile della cancelleria è tenuto a controllare che il contenuto del fascicolo d'ufficio su supporto cartaceo sia presente nel fascicolo informatico.

17. *Trasmissione della sentenza.*

1. La trasmissione per via telematica della minuta della sentenza o della sentenza stessa, redatte come documenti informatici sottoscritti con firma digitale, è effettuata, ai sensi dell'articolo 119 delle norme di attuazione del codice di procedura civile, con particolari modalità stabilite con il decreto di cui all'articolo 3, comma 3, e dirette ad assicurarne l'integrità, l'autenticità e la riservatezza.
2. Il cancelliere, ai fini del deposito della sentenza ai sensi dell'articolo 133 del codice di procedura civile, sottoscrive la sentenza stessa con la propria firma digitale.

18. Informatizzazione del processo amministrativo e contabile.

1. Le disposizioni del presente regolamento si applicano, in quanto compatibili, anche al processo amministrativo e ai processi innanzi alle sezioni giurisdizionali della Corte dei conti.

2. Con decreti del Presidente del Consiglio dei Ministri, sentita l'Autorità per l'informatica nella pubblica amministrazione, sono stabilite le regole tecnico-operative per il funzionamento e la gestione del sistema informatico della giustizia amministrativa e contabile. I decreti sono adottati entro il termine di cui all'articolo 19, comma 2.

19. Disposizioni finali.

1. Le disposizioni del presente regolamento si applicano ai giudizi iscritti a ruolo dopo il 1° gennaio 2002.

2. Il decreto ministeriale previsto dall'articolo 3, comma 3, è adottato entro il 30 ottobre 2001.

CAPITOLO III

REATI INFORMATICI

La diffusione delle nuove tecnologie informatiche e telematiche ha dato luogo a nuove ipotesi criminose ponendo numerose problematiche giuridiche anche relative alle responsabilità dei soggetti coinvolti nello scambio di dati, informazioni e notizie pubblicate su siti web.

In un primo momento il giurista si è opposto a una indiscriminata estensione delle figure criminose tradizionali alle nuove condotte riaffermando il principio "nullum crimen, nulla poena sine lege", già formulato nel diritto romano e codificato in tutti i Paesi dell'Europa occidentale, ad esempio con l'art. 1 del codice penale italiano, l'art. 4 del codice penale francese e l'art. 103, II comma, della Costituzione della Repubblica Federale di Germania.

Negli anni ottanta vi è stato un intervento del legislatore che, qualificando espressamente alcuni reati alcune forme di abusi informatici, ha posto o ha tentato di porre fine alle controversie della dottrina e alle incertezze della giurisprudenza e ha soddisfatto un'esigenza punitiva sempre più sentita dalla società nei confronti delle nuove forme di finalità.

Nel Regno Unito è stato emanato il Forgery and Counterfeiting Act nel 1981 negli Stati Uniti d'America il Federal Counterfeit Access Device and Computer Fraud and Abuse nel 1984, in Germania la seconda legge per la prevenzione dei reati economici del 1986, e in Francia la legge n. 88-19 relativa alla frode informatica. In Italia, dopo la legge 18 maggio 1978 in materia di danneggiamento degli impianti e la legge 321 del 1981, istitutiva del Centro elaborazione dati presso il Ministero dell'Interno, sono state emanate norme in materia di reati informatici soltanto negli anni '90. Così, ad esempio, l'art. 12 della legge 5 luglio 1991 n. 197 che punisce l'uso indebito di carte di credito; l'art. 10 della legge n. 518 del 1992 in materia di diritto di autore sui programmi per l'elaboratore; e infine la legge 23 dicembre 1993 n. 547contenente modificazioni ed integrazioni alle norme del codice penale in tema di criminalità informatica. Quest'ultima legge può essere considerata come un tentativo

del legislatore italiano di dettare una disciplina generale dei reati informatici. A tal fine il legislatore ha ritenuto che le nuove figure di reato non dovessero essere inserite in un apposito titolo del libro secondo del codice penale e che fosse, invece, preferibile "ricondurre i nuovi reati alle figure già esistenti che ad esse, pur nella loro autonomia appaiono più vicine". In particolare, il legislatore ha ritenuto preferibile questa soluzione per la convinzione che la particolarità della materia non costituisse ragione sufficiente per la configurazione di uno specifico titolo; il codice penale infatti raggruppa i reati in base all'unità dell'oggetto giuridico, mentre le figure da introdurre sono apparse soltanto "quali nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica ecc.) già oggetto di tutela nelle diverse parti del corpo del codice" (dalla relazione al disegno di legge).

Le innovazioni più rilevanti, introdotte dalla su esposta normativa, sono sintetizzabili nei seguenti punti:

- *a) introduzione del concetto di violenza informatica, previsione dei correlativi reati e, in particolare, dell'esercizio arbitrario delle proprie ragioni (art. 392, terzo comma), dell'attentato a impianti di pubblica utilità (art. 420).Quest'ultima rientra fra le fattispecie a consumazione anticipata, si tratta cioè di una fattispecie criminosa nella quale il momento consumativo coincide con l'azione stessa senza la necessità che si produca un evento,*
- *b) danneggiamento dei sistemi informatici e telematici (art. 635 bis,); d diffusione dei programmi diretti a danneggiare o a interrompere il sistema informatico (art. 615 quinquies);*
- *c) configurazione del nuovo reato di accesso abusivo a un sistema informatico o telematico (art. 615 ter) e di detenzione e diffusione abusiva di codici di acceso a sistemi informatici (art. 615 quater);*
- *d) configurazione del nuovo reato di frode informatica (art. 640 ter);*
- *e) introduzione del delitto di falso su documento informatico (art. 491 bis);*
- *f) estensione della nozione di corrispondenza in tema di delitti contro l'inviolabilità dei segreti da quella originaria epistolare, telegrafica e telefonica a quella informatica o telematica e a qualunque altra*

trasmissione a distanza di suoni, immagini o di altri dati (art. 616, art. 617 quater, art. 617 quinquies e sexies, art. 621, art. 623 bis del codice penale, art. 266 bis e 268 del codice di procedura penale.)

Successivamente, in tema di reati informatici, sono intervenute leggi speciali dirette a tutelare beni informatici, che hanno previsto nuove figure di ipotesi delittuose. Va ricordato a questo proposito la legge sulla tutela penale dei programmi del 1992 integrata dalla recente legge 18 agosto 2000 n. 248, la legge sulla sottoscrizione elettronica del 31 dicembre 1996 n. 675, la legge sulla tutela dei dati personali del 1996 , la legge sulla tutela delle banche di dati del 6 maggio1999 n. 169 e infine il d.lgs. 9-4-2003 n. 68 di attuazione della direttiva 2001/29/CE sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione.

Quindi si è delineato un panorama di norme in tema di reati informatici molto ampio e variegato: dalla tutela dei dati personali all'accesso e alle intercettazioni abusive; dalla tutela penale dei programmi delle banche di dati e dei chip al furto informatico e ai danneggiamenti informatici; dalla induzione in errore di un elaboratore al falso informatico. La comunità scientifica si è soffermata sull'analisi delle singole fattispecie criminose che incidono sui beni informatici nelle varie esperienze legislative degli Stati membri Europei nell'intento di realizzare una disciplina quanto più uniforme possibile. Accanto a questo compito, di per sé di grande importanza, vi è poi l'esigenza di ricondurre a unità le varie figure criminose: di vedere, cioè, se si tratti di una categoria meramente descrittiva,ovvero di una categoria unitaria caratterizzata da una disciplina sua propria e da un suo proprio oggetto giuridico. Un ulteriore problematica riguarda l'accertamento e la prevenzione dei reati

Infatti si verifica spesso che la diffusione di un fenomeno delittuoso, come ad esempio la pirateria informatica, induca il legislatore a comminare sanzioni estremamente severe. Una severità che ha una duplice ragione: da una parte la necessità di tutela delle case produttrici dei beni informatici, dall'altra la difficoltà di accertamento e di prevenzione di questi reati.

La dottrina, a tal proposito si è chiesta se ciò sia opportuno e giustificato; se non si debbano percorrere altre strade; se non sia necessario cioè rivedere, alla luce delle

nuove tecnologie, istituti tradizionali. Se, ad esempio, si debba continuare a configurare il diritto di autore come diritto di riproduzione di copie cartacee in un momento in cui il nuovo libro è scritto in bit.

La ricerca può condurre quindi a risultati ancora più ampi di quelli strettamente penali: un nuovo concetto di diritto di autore che tenga conto della necessità e della facilità di riproduzione dei programmi e della necessità di utilizzazione di essi per un continuo progresso tecnologico; un nuovo concetto di libertà personale basato sull'autodeterminazione informativa intesa come potere di controllo dell'individuo sui propri dati personali; un nuovo concetto di documento scritto, svincolato dal supporto materiale e dalla localizzazione territoriale, un documento che non conosca distinzione tra atti originali e copie; un nuovo concetto di atto di disposizione patrimoniale basato su trasferimenti elettronici di fondi e non su consegne materiali di danaro o di titoli di credito.

In questo capitolo sono affrontate anche le questioni giuridiche emerse a seguito della diffusione della rete internet quali, ad esempio, la responsabilità del provider (Ente che fornisce a terzi accessi ad Internet, gratuitamente o a pagamento).
La problematica sorta a tale proposito riguardava la delimitazione dell'area «oggettiva» dell'illecito per il settore Internet: era necessario tipizzare comportamenti ed attività reputati socialmente rilevanti.

In quest'ottica, tanto per semplificare il discorso, si è distinta, ai fini della individuazione del regime di responsabilità applicabile agli Internet provider, una memorizzazione temporanea dei dati presenti on line, da un'altra di tipo durevole.

Con riguardo a quest'ultimo servizio, da un lato viene sancita la regola generale (art. 15, direttiva 31/2000/CE) in base alla quale il provider (detto, in tal caso, hosting provider) non è ritenuto civilmente responsabile per il contenuto delle informazioni immesse on line dal proprio cliente; dall'altro (ex art. 14, della citata direttiva n. 31/2000) si prevede però che il provider stesso debba solidalmente rispondere con il proprio cliente dei danni da quest'ultimo cagionati ai terzi, qualora; a) non abbia agito per «arginare» i suddetti pregiudizi, pur essendo stato reso edotto (anche da parte del presunto offeso) della illiceità delle informazioni presenti (suo tramite) on line; oppure

ancora, b) sia da ritenersi comunque consapevole di fatti, o circostanze, che rendevano manifesta la suddetta illiceità.

Infine, un tema connesso all'uso delle tecnologie informatiche particolarmente rilevante per un giurista, attualmente oggetto di interventi legislativi e approfondimenti giurisprudenziali è il fenomeno dello "spamming".

In particolare lo spamming è un'attività suscettibile di avere ripercussioni anche in sede penale, oltre che in sede civile, anche se il reato di spamming appare di non immediata individuazione e di difficile realizzazione.

La condotta del reato potrebbe essere riconducibile all'art. 167[1] *del Codice Privacy, una norma incriminatrice che descrive gli elementi del reato di trattamento illecito di dati personali.*

Gli elementi costitutivi della fattispecie criminosa sono molteplici, e devono tutti necessariamente concorrere ai fini della configurazione del fatto reato.

V'è innanzitutto una salvezza nell'incipit del primo comma alla circostanza in cui «il fatto costituisca più grave reato» che è idonea ad escludere la configurabilità del reato di cui all'art. 130 del codice e quindi l'applicabilità dell'istituto penalistico che abbiamo chiamato "reato di spamming". In secondo luogo, quanto all'elemento soggettivo del reato, esso è indubbiamente da ravvisarsi nel dolo specifico, che può consistere nel fine di trarre per sé o per altri profitto, da un lato, oppure di recare ad altri un danno.

Sul termine "profitto" è opportuno ricordare quanto affermato dalla sentenza della Cassazione penale, n. 33816/2001 (alla quale si sono uniformate le prevalenti sentenze successive in materia di contraffazione di software): mentre lo scopo di lucro identifica la finalità di perseguire un vantaggio di tipo patrimoniale, il termine profitto viene definito come «giovamento, vantaggio, beneficio, sia pratico sia intellettuale o morale». Invece il fine di recare ad altri danno descrive una volontà criminosa di

[1] Art. 167 del D.Lgs. n. 196/2003: (Trattamento illecito di dati)« 1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

realizzare una lesione giuridicamente rilevante della sfera non solo patrimoniale, ma anche morale, di un'altra persona.

Proseguendo nella lettura della norma, la condotta incriminata è descritta dalla violazione delle disposizioni di cui all'art. 130 del Codice Privacy, ovvero la disciplina circa l'invio di comunicazioni non desiderate.

Infine la norma ha introdotto un ulteriore elemento costitutivo della fattispecie criminosa, in mancanza del quale, il reato non può dirsi configurato: la realizzazione di un nocumento per l'interessato[2]*.*

La terza sezione penale della Cassazione, con la sentenza 28/05-9/07 2004, n. 1134 (30134/2004), ha affermato che – in relazione alla nozione di "nocumento"- «devono essere senza dubbio escluse le semplici violazioni formali ed irregolarità procedimentali, ma anche quelle inosservanze che producano un 'vulnus' minimo all'identità personale del soggetto ed alla sua privacy […] sia nell'aspetto negativo sia positivo e non determinino alcun danno patrimoniale apprezzabile».

In un'altra occasione, sentenza Cass., sez. III pen. n. 26680/2004, è stato ritenuto sussistente il nocumento in relazione alla «lesione della tranquillità e dell'immagine sociale» subita da un'interessata in conseguenza della condotta dell'ex fidanzato, il quale aveva diffuso sul web immagini della donna tratte da una videocassetta contenente un suo spogliarello, unitamente al suo numero telefonico.

In base ad un'altra pronuncia della Cassazione (Cass., sez. III pen., sent. 17/11/2004-15/02/2005 n. 5728) è stato elaborato un principio in base al quale l'utilizzazione di dati personali rinvenuti liberamente sul web non costituisca una fattispecie di trattamento senza consenso in quanto in internet i dati sono reperibili alla stregua di quanto accade per i dati tratti da pubblici registri, pubblici elenchi etc. «Non sarebbe pertanto configurabile la violazione di quanto disposto dall'art. 23», secondo questa sentenza, e quindi non sarebbe nemmeno configurabile la sussistenza del reato di cui all'art. 167, comma 1, D.L.vo 196/2003.

Inoltre, un'altra e recentissima sentenza del Tribunale penale di Udine ha ritenuto non ravvisabile il nocumento in caso di un unico messaggio pubblicitario inviato che, data la sua non ripetitività, avrebbe causato una lesione minima della privacy del destinatario.

[2] In argomento sul sito www.anti-phishing.it è pubblicato un articolo di Luca Bovino dal titolo "Lo spamming come illecito penale" nel quale sono elencate le principali pronunce relative al reato qui in esame.

Per completezza di discorso, occorre ricordare che le sanzioni previste dall'articolo 130 del Codice Privacy sono la reclusione da sei a diciotto mesi, oppure, se il fatto consiste nella comunicazione o nella diffusione, con la reclusione da sei a ventiquattro mesi.

Lo spamming, nell'ordinamento italiano, costituisce anche un illecito civile come si evince soprattutto due sentenze del Giudice di Pace di Napoli, rispettivamente del 7 e del 26 giugno 2004 .

In queste due pronunce il giudice ha ricondotto l'attività di spamming nell'ambito della responsabilità extracontrattuale, ai sensi dell'art. 2043 del codice civile.In particolare in entrambe le sentenze lo spammer è stato condannato a cancellare i dati del ricorrente dai propri archivi elettronici nonché a risarcire i danni non patrimoniali in conseguenza dell'ingiusto turbamento arrecato alla vita privata del destinatario del messaggio pubblicitario.

Il giudice di pace ha affermato che il danno di natura patrimoniale si identifica con le «spese generali, gli inconvenienti e le perdite di tempo subite», mentre il danno non patrimoniale è quantificato tenendo conto « del danno alla vita di relazione del danno esistenziale conseguente alla lesione e al turbamento della qualità di vita dell'attore». In questo modo anche il danno da spamming rientra nel cosiddetto danno esistenziale, categoria di recente elaborazione giurisprudenziale.

Occorre precisare che le due sentenze napoletane facevano riferimento a controversie sorte nel 2003, ovvero prima dell'entrata in vigore del Codice sulla protezione dei dati personali che risale al primo gennaio 2004.

Nell'attuale panorama normativo il giudice competente per le controversie inerenti le violazioni del suddetto codice è il tribunale in composizione monocratica, ed il foro competente è quello del titolare del trattamento dei dati (ai sensi dell'art. 152 del D.Lgs. 196/2003)[3]. Inoltre, a differenza dei casi che hanno interessato i due giudici campani, l'atto introduttivo del giudizio non è la citazione bensì il ricorso.

[3] dell'art. 152 del D.Lgs. 196/2003(Autorità giudiziaria ordinaria) "1. Tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del presente codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'autorità giudiziaria ordinaria.
2. Per tutte le controversie di cui al comma 1 l'azione si propone con ricorso depositato nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento.
3. Il tribunale decide in ogni caso in composizione monocratica.
4. Se è presentato avverso un provvedimento del Garante anche ai sensi dell'articolo 143, il ricorso è proposto entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito. Se il ricorso è proposto oltre tale termine il giudice lo dichiara inammissibile con ordinanza ricorribile per cassazione.

A tal proposito è utile ricordare la nota alle due sentenze qui citate, reperibile all'indirizzo: http://www.anti-phishing.it/spamming/spamming.responsabilita.civile.php, in cui si sottolinea come le pronunce si distinguono poiché ricollegano la responsabilità civile connessa all'attività di spamming all'ambito della responsabilità extracontrattuale (art. 2043 del codice civile), piuttosto che a quello della responsabilità connessa allo svolgimento di attività pericolose (art. 2050 codice civile), come peraltro era già previsto dall'art. 18 della legge n. 675/96, prima dell'entrata in vigore dell'art. 15 del Codice.

Tale precisazione riveste particolare interesse infatti, se si riconduce la responsabilità civile dello spammer nell'ambito della responsabilità extracontrattuale, l'onere probatorio ricade sul soggetto che voglia agire in giudizio contro lo spamming subito. Questi pertanto è tenuto a dimostrare i danni subiti (anche se di natura non patrimoniale), la colpa o il dolo dello spammer, nonché il nesso di causalità fra l'azione colposa o dolosa dello spammer ed il danno subito da egli subito.

---

5. La proposizione del ricorso non sospende l'esecuzione del provvedimento del Garante. Se ricorrono gravi motivi il giudice, sentite le parti, può disporre diversamente in tutto o in parte con ordinanza impugnabile unitamente alla decisione che definisce il grado di giudizio.
6. Quando sussiste pericolo imminente di un danno grave ed irreparabile il giudice può emanare i provvedimenti necessari con decreto motivato, fissando, con il medesimo provvedimento, l'udienza di comparizione delle parti entro un termine non superiore a quindici giorni. In tale udienza, con ordinanza, il giudice conferma, modifica o revoca i provvedimenti emanati con decreto.
7. Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni.
8. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impe-dimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.
9. Nel corso del giudizio il giudice dispone, anche d'ufficio, omettendo ogni formalità non necessaria al contraddittorio, i mezzi di prova che ritiene necessari e può disporre la cita-zione di testimoni anche senza la formulazione di capitoli.
10. Terminata l'istruttoria, il giudice invita le parti a precisare le conclusioni ed a proce-dere, nella stessa udienza, alla discussione orale della causa, pronunciando subito dopo la sentenza mediante lettura del dispositivo. Le motivazioni della sentenza sono depositate in cancelleria entro i successivi trenta giorni. Il giudice può anche redigere e leggere, unitamente al dispositivo, la motivazione della sentenza, che è subito dopo depositata in cancelleria.
11. Se necessario, il giudice può concedere alle parti un termine non superiore a dieci giorni per il deposito di note difensive e rinviare la causa all'udienza immediatamente successiva alla scadenza del termine per la discussione e la pronuncia della sentenza."
12. Con la sentenza il giudice, anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), quando è necessario anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile, accoglie o rigetta la domanda, in tutto o in parte, prescrive le misure necessarie, dispone sul risarcimento del danno, ove richiesto, e pone a carico della parte soccombente le spese del procedimento.
13. La sentenza non è appellabile, ma è ammesso il ricorso per cassazione.
14. Le disposizioni di cui al presente articolo si applicano anche nei casi previsti dall'articolo 10, comma 5, della legge 1° aprile 1981, n. 121, e successive modificazioni.»]

Viceversa, inquadrando la responsabilità civile dello spammer nell'ambito dell'art. 2050 c.c., sul soggetto che agisce in giudizio grava soltanto l'onere di dimostrare i danni subiti (che anche in questo caso potrebbero essere di natura non patrimoniale) e il nesso di causalità fra il danno subito e l'azione dello spammer. Tale ultima ricostruzione appare maggiormente convincente, anche in considerazione del fatto che lo svolgimento di un'attività di trattamento di dati personali (qual è, per l'appunto, l'attività di e-mail spamming) è considerata dal codice un'attività pericolosa, stante il rinvio, contenuto nell'art. 15 del D.Lgs. 196/2003[4]*, all'art. 2050 del codice civile.*

[4] Art. 15 «(Danni cagionati per effetto del trattamento) 1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. 2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.»;

Il Parlamento europeo non approva la Proposta di direttiva del Parlamento europeo e del Consiglio relativa alla brevettabilità delle invenzioni attuate per mezzo di elaboratori elettronici.

NUMERO SCHEDA: 6404

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

FONTE: INTERLEX

NATURA ATTO: PROPOSTA DI DIRETTIVA

Con seicentoquarantotto "no", quattordici "sì" e diciotto astenuti è stata "bocciata" dal Parlamento europeo la Proposta di direttiva del Parlamento europeo e del Consiglio relativa alla brevettabilità delle invenzioni attuate per mezzo di elaboratori elettronici, nota come "direttiva sulla brevettabilità del software".
A tal proposito interessante è il commento del relatore della proposta, il francese Michel Rocard che afferma: "Si è arrivati a questo voto con posizioni diverse, ma c'è una collera collettiva e unanime per l'atteggiamento della Commissione e del Consiglio che hanno mostrato totale disprezzo e sarcasmo nei confronti delle scelte fatte dal Parlamento europeo in prima lettura".
Una delle organizzazioni, che ha esposto più volte le ragioni del "no" , la Free Software Foundation Europe , chiede un cambiamento delle politiche dell'Ufficio europeo dei brevetti (EPO). E' noto, infatti, che negli ultimi anni l'EPO ha allargato le maglie della brevettabilità del software, seguendo la linea dettata dagli Stati Uniti e contro i principi accettati a livello internazionale (vedi I brevetti software sono contro la Costituzione europea di Nicola Walter Palmieri).

Il Tribunale di Rovereto si pronuncia in materia di accesso abusivo ad un sistema informatico o telematico.

NUMERO SCHEDA: 6320

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

FONTE: DIRITTO PENALE E PROCESSO

AUTORE: Roberto Flor

NUMERO: 1

DATA: 31/01/2005

PAGINA: 81-94

RIFERIMENTO NORMATIVO: art. 615 - ter del codice penale

NATURA ATTO: SENTENZA

DATA ATTO: 09/01/2004

NUM. ATTO: 343

ORGANO: TRIBUNALE

Con sentenza n. 343/2004 il Tribunale di Rovereto ha affermato che non è configurabile il reato previsto dall'art. 615- ter del codice penale (accesso abusivo ad un sistema informatico o telematico) nel fatto di chi si limiti ad accedere ad una parte del sistema comune a tutti i dipendenti dell'impresa, cui ha parimenti diritto, a nulla rilevando che in quello spazio informatico, per errore, per la condotta illecita di terze persone o per qualsiasi altra causa vi fossero collocati anche dati riservati del titolare, e che l'imputato li abbia visualizzati o duplicati.
Il bene giuridico protetto dalla norma di cui all'art. 615-ter c.p. è il "domicilio informatico" che non può considerarsi una mera specificazione del domicilio tutelato dall'art. 614 c.p., ma deve essere inteso quale proiezione spaziale della persona indicante un nuovo bene protetto, la "riservatezza informatica", che in concreto si risolve nell'indisturbata fruizione del sistema informatico o telematico.
Presso il settore Studi e documentazione legislativi è consultabile, sulla rivista "Diritto penale e processo", n. 1/2005, il testo della sentenza.
Sempre sulla stessa rivista è consultabile un interessante commento alla sentenza, ricco di riferimenti legislativi, giurisprudenziali e dottrinali, a cura di Roberto Flor, intitolato: "*Per la consumazione del reato di accesso abusivo ad un sistema informatico o telematico non è necessario il superamento delle misure di sicurezza (manifestazione dello ius excludendi alios), a condizione che sul piano formale esse esistano*".
Il commento, dopo una breve premessa, affronta i seguenti temi:

- "Il bene giuridico protetto dall'art. 615-ter c.p.".
- "L'abusività dell'accesso e l'individuazione della persona offesa dal reato".
- -"Le misure di sicurezza, la manifestazione dello ius excludendi alios e la consumazione del reato".
- "Il rapporto fra la previsione dell'art. 615-ter c.p. e il "Codice in materia di protezione dei dati personali": ambito di tutela e misure protettive".
- "Conclusioni".

La responsabilità dei motori di ricerca rispetto all'illiceità delle informazioni contenute nei siti memorizzati.

NUMERO SCHEDA: 6163

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

NATURA ATTO: COMMENTO

Negli ultimi anni il diffondersi dell'informatica ha suscitato una serie di problematiche giuridiche legate alla responsabilità dei motori di ricerca che, sinteticamente, possono essere considerati delle banche - dati finalizzate ad indicizzare i testi presenti in rete per facilitarne la consultazione da parte degli utenti.
L'indicizzazione dei testi avviene in modo automatico tramite appositi *software* e, dunque, in via generale i motori di ricerca non sono responsabili per l'illiceità delle informazioni contenute nei siti indicizzati.
Tuttavia l'articolo 15, dlgs. 70/2003, attuazione della direttiva comunitaria n. 31 del 2000 , pur ribadendo il suindicato principio generale impone al gestore del motore di ricerca l'obbligo di cancellare, anche a posteriori, i documenti temporaneamente memorizzati nel caso in cui venga a conoscenza della loro illiceità.
Più precisamente tale articolo afferma testualmente che: *"nella prestazione di un servizio della società dell'informazione, consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, il prestatore non è responsabile della memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta, a condizione che: (...omissis...)*
e) agisca prontamente per rimuovere le informazioni che ha memorizzato, o per disabilitare l'accesso, non appena venga effettivamente a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione."
Un secondo ordine di problemi concerne la violazione del diritto d'autore in relazione ai documenti ipertestuali oggetto di indicizzazione.La soluzione a cui si è pervenuti distingue il caso in cui per rappresentare il link si utilizzi il materiale protetto da copyright, senza consenso del titolare del diritto, incorrendo così nella violazione del diritto d'autore, dal caso in cui, al contrario, il link è utilizzato in quanto collegamento, senza copiatura del contenuto del sito linkato.In tale ultimo caso il motore di ricerca è esonerato da ogni responsabilità.

Un interessante articolo in materia di "spamming".

NUMERO SCHEDA: 6124

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

FONTE: LA NUOVA GIURISPRUDENZA CIVILE COMMENTATA

AUTORE: Paola Crugnola

NUMERO: 3

DATA: 30/06/2005

PAGINA: 474-479

NATURA ATTO: COMMENTO

E' un articolo sintetico e molto chiaro intitolato "Disciplina dello *spamming*", a cura di Paola Crugnola.
Spamming o *spam* è, come lo definisce l'autrice, un problema particolarmente grave della pubblicità elettronica consistente nell'invio simultaneo di messaggi (prevalentemente pubblicitari) non sollecitati ad un gran numero di destinatari.
Il commento, particolarmente ricco di riferimenti dottrinali, normativi e giurisprudenziali, si articola nei seguenti capitoli:
1. Lo *spamming*: caratteristiche generali.
2. *Spamming* commerciale: disciplina comunitaria e nazionale.
3. *Spamming* e interventi del Garante per la protezione dei dati personali.
4. *Spamming* per fini di propaganda elettorale.
5. Necessità di una collaborazione internazionale per combattere lo *spamming*.
L'articolo è consultabile presso il settore Studi e documentazione legislativi.

Il Tribunale di Catania ha stabilito la responsabilità del provider per la pubblicazione di un'opera, senza il benestare dell'autore, su un sito Internet, realizzato e gestito per conto di un Comune.

NUMERO SCHEDA: 5171

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

FONTE: WWW.FILODIRITTO.IT

NATURA ATTO: SENTENZA

DATA ATTO: 29/06/2004

NUM. ATTO: 2286

Secondo il Tribunale di Catania, in riferimento alla pubblicazione di un'opera, senza il benestare dell'autore, su un sito Internet realizzato e gestito per conto di un Comune, il provider è responsabile dell'illecito posto in essere dall'utilizzatore allorchè abbia piena consapevolezza del carattere antigiuridico dell'attività svolta da quest'ultimo. La responsabilità del provider è soggettiva e può essere colposa se il fornitore del servizio , consapevole della presenza sul sito di materiale sospetto, si astenga dall'accertarne l'illiceità e dal rimuoverlo. E' dolosa quando egli sia consapevole anche dell'antigiuridicità della condotta dell'utente e ometta di intervenire.
La responsabilità del provider è subordinata alla circostanza che questi sappia della illiceità dell'attività o dell'informazione o anche dell'esistenza dell'attività o dell'informazione.

Si allega copia della sentenza del Tribunale di Catania, Sez. IV Civ., 25-29 Giugno 2004, n. 2286.

Sentenza.

Giudice Dr. Mariano Sciacca

Svolgimento del processo

Con atto di citazione notificato il 19.10.2001 V. K. conveniva in giudizio la società cooperativa a r.l. X. L., all'uopo, esponendo:

- Che la società convenuta forniva al comune di N. un servizio di hosting sul sito internet www.cormorano.net, giusta deliberazione della Giunta Municipale n. 222 del 15.4.1998;
- Che nel detto sito internet veniva indebitamente utilizzata l'opera intellettuale di esso attore, già edita con la pubblicazione "N. guida storico-turistica";
- Che, nonostante apposita diffida inviata alla cooperativa convenuta, questa aveva continuato ad utilizzare la propria opera;
- Che il Comune di N. aveva inutilmente richiesto l'oscuramento delle pagine internet in questione;
- Che tale comportamento integrava un illecito civile da risarcirsi nella misura di £. 80.000.000.

Chiedeva conseguentemente dichiararsi l'indebito utilizzo da parte della convenuta della propria opera intellettuale e per l'effetto condannarsi la stessa a cessare l'illecito utilizzo e a pagare a titolo di risarcimento dei danni patiti la somma di E. 41.316,55 o in quella quantificata secondo equità dal giudice. Con interessi legali dal 12.1.20012 al soddisfo.

Iscritta la causa a ruolo, si costituiva la cooperativa X. L. a r.l., la quale deduceva il proprio difetto di legittimazione passiva e, nel merito, l'infondatezza della domanda attorea. Con vittoria di spese e compensi.

Con memoria ex art. 183, comma quinto, c.p.c. parte attrice dichiarava limitarsi la dichiarazione di responsabilità della convenuta all'indebito utilizzo dell'opera intellettuale per il periodo di tempo compreso tra l'agosto 1998 e il febbraio 2001.

Indi, istruita la causa e precisate le conclusioni, all'udienza del 15.3.2004 la causa veniva posta in decisione con l'assegnazione dei termini di rito.

Motivi della decisione

Preliminarmente va esaminata l'eccezione di difetto di legittimazione passiva della cooperativa a r.l. X. L., la quale ha dedotto - in comparsa di costituzione - di avere già "oscurato" il sito dedicato al Comune di N., operante sotto il dominio "Il riflettore.it", subito dopo la ricezione della formale diffida da parte dell'attore nel gennaio 2001, nonché essere stato successivamente registrato sempre per il Comune di N. un nuovo sito sotto il distinto dominio "cormorano.net" a nome di società diversa dall'odierna convenuta, cioè la C. N. s.a.s..

L'eccezione è solo parzialmente fondata proprio alla luce delle difese spiegate dalla convenuta, la quale, per sua espressa ammissione ha gestito sotto il dominio "Ilrifelttore.it" il sito del comune di N. almeno sino al gennaio 2001, sicchè limitatamente al periodo intercorrente tra l'agosto del 1998 – momento iniziale di apertura del sito del Comune di N. - e il gennaio del 2001 sussiste certamente tanto - in ipotesi - la legittimazione della convenuta quanto, nel merito, la titolarità passiva del relativo rapporto controverso relativamente agli esposti fatti costituenti violazione del diritto di autore dell'odierno attore.

Peraltro è a notare che, proprio in conseguenza delle difese esposte dalla convenuta in comparsa responsiva, l'attore - con memoria autorizzata ex art. 183 quinto comma c.p.c., ha espressamente modificato la domanda chiedendo il risarcimento del danno patito per l'indebito utilizzo dell'opera intellettuale "nella misura ritenuta equa e giusta dal giudice.".

Tanto premesso, va, in primo luogo, rilevato come nessuna contestazione sia sorta in ordine alla paternità in capo al V. K. dell'opera storiografica relativa al "Profilo storico" del Comune di N. (v. la pubblicazione in atti prodotta dall'attore "Guida storico-turistica del Comune di N.") e alla conseguente titolarità in capo allo stesso dei diritti di natura patrimoniale e morale inerenti l'opera dell'ingegno dallo stesso realizzata.

L'art. 12 della legge del 1941 sul diritto di autore chiarisce che "l'autore ha diritto di utilizzare economicamente l'opera in ogni forma e modo, originale e derivato, nei limiti fissti da questa legge e, in particolare, con l'esercizio dei diritti esclusivi indicati negli articoli seguenti".

A tal riguardo è noto che i diritti esclusivi individuati dalla legge dagli artt. 13-19 hanno contenuto patrimoniale, tutti essi implicando e comportando il diritto dell'autore di disporre matrimonialmente degli stessi, tramite il rilascio di licenze e autorizzazioni variamente atteggiate per il conferimento in uso dell'opera ovvero la cessione dei diritti medesimi a terzi.

Da tale ambito va poi tenuto distinto il profilo relativo al diritto morale di autore, alla paternità e integrità dell'opera, al diritto di pubblicazione e di cd. pentimento, i quali tutti si caratterizzano e rilevano quali espressione della personalità dell'autore e della personalizzazione conseguente dell'opera.

Per quanto concerne poi l'utilizzazione in rete delle opere tutelate dalla normativa in esame, occorre rilevare come i file contenenti testi scritti, rinvenibili nella rete telematica in veste elettronica, godono senza dubbio della medesima protezione e tutela delle opere letterarie tradizionali in cui sono sempre convertibili, attraverso la stampa su materiale cartaceo, trattandosi comunque di attività intellettuale dell'uomo, a prescindere dalla natura del supporto veicolare dell'espressione artistica e dal giudizio di valore sull'apporto artistico.
Venendo quindi ai profili "patologici" rilevanti nel caso di specie, è da rilevare come l'illecito civile on line può derivare dalla violazione delle norme a tutela del diritto d'autore, dalla violazione del diritto alla riservatezza o di altri diritti della persona, come l'onore o la reputazione, dalla violazione delle norme a tutela dei marchi, dalla violazione delle norme in materia di concorrenza sleale. D'altronde, posto che la rete è in grado di ospitare dati ed informazioni di ogni tipo, è del tutto naturale che sulla rete o, meglio, attraverso la rete, possano essere consumati tutti gli illeciti che si fondano sulla diffusione o sulla utilizzazione di dati o informazioni.
Autorevole dottrina ha, a tal uopo, notato come la ragione sostanziale che ha indotto nel recente passato la prassi giudiziaria e legale ad individuare proprio nell'Internet provider, e cioè nel soggetto che fornisce a terzi l'accesso alla rete telematica, il corresponsabile delle violazioni commesse per mezzo della rete da un qualsiasi utente sul suo server debba essere nella concreta necessità di selezionare concretamente almeno un soggetto responsabile della violazione a fronte della volatilità e, a volte, inafferabbilità degli originari autori dell'illecito stesso, sub specie di committenti per la pubblicazione sul www. Considerazione di natura sostanzialistica, la quale deve, peraltro, confrontarsi con le esigenze di certezza del diritto, dei traffici commerciali e di personalità dell'illecito che non possono non rilevare anche sul versante civilistico in esame. A tal riguardo è noto come, tanto in dottrina che in giurisprudenza, si sia prospettato, quanto alla posizione del provider al quale vengano contestati fatti costituenti illecito extracontrattuale, il ricorso a modelli di estensione soggettiva della responsabilità civile, come, ad esempio, la possibilità di ritenere analogicamente applicabile al provider la figura del responsabile editoriale di una testata giornalistica o quella, del tutto affine, dell'editore televisivo. In tal senso, equiparandosi il gestore di un sito Internet ad un responsabile editoriale, si è così ritenuto possibile ipotizzare l'applicazione delle norme (art. 57 c.p.) sui reati commessi a mezzo di stampa e attribuire al provider l'obbligo di verificare la legittimità di tutto il materiale pubblicato sul proprio server, compreso quello inviato da terzi.
In quest'ottica, il provider diverrebbe corresponsabile dell'illecito del terzo utente sulla base di una culpa in vigilando, consistente nel mancato adempimento dell'obbligo di controllo del materiale inviato sul proprio server (Tribunale di Napoli - caso "Cirino Pomicino - ord. 8 agosto 1996, ove si è affermata la responsabilità civile del provider per aver "autorizzato, consentito, o comunque agevolato il comportamento illecito" di un utente colpevole di aver diffuso in rete messaggi promozionali contenenti nomi e marchi appartenenti a società concorrenti, sul presupposto che della compartecipazione colposa per il provider, assimilabile ad un responsabile editoriale, in quanto "il proprietario di un canale di comunicazione destinato a un pubblico di lettori - al quale va equiparato quale organo di stampa un sito Internet - ha l'obbligo di vigilare sul compimento di atti di concorrenza sleale eventualmente perpetrati attraverso la pubblicazione di messaggi pubblicitari di cui deve verificare la natura palese, veritiera e corretta, concorrendo, in difetto, e a titolo di responsabilità aquiliana, nell'illecito di concorrenza sleale" (di analogo tenore: Tribunale di Napoli, 8 agosto 1998 - che ha assimilato il gestore di Rete ad un organo di stampa, con conseguente obbligo di controllo sui contenuti del sito web - Tribunale di Macerata, 2 dicembre 1998, Tribunale di Teramo, 11 dicembre 1997; Tribunale di Bologna 26 novembre 2001, ove si afferma la responsabilità del provider in virtù dell'applicabilità in via analogica dell'art. 11 L.47/48, secondo il quale "per i reati commessi col mezzo della stampa sono civilmente responsabili, in solido con gli autori del reato e fra di loro, il proprietario della pubblicazione e l'editore".).
La riferita linea interpretativa è stata, ad avviso del giudicante, correttamente oggetto di puntuali critiche in dottrina e poi in giurisprudenza, denunziandosi come irrealistica l'affermazione di una "colpa/negligenza" del provider per l'impossibilità pratica di controllare ogni messaggio inviato su un server nonché rendendo evidenti le differenze di tali ipotesi rispetto a quelle contemplate dalla legge sull'editoria che renderebbero inapplicabile analogicamente la suddetta disciplina al caso in esame.
Segnatamente va rilevato come affermare una responsabilità per omesso controllo del provider, in un campo dove è materialmente impossibile operare una verifica dei dati trasmessi da tutto il mondo, equivarrebbe ad introdurre una nuova ed inaccettabile ipotesi di responsabilità oggettiva - che prescinde dalla colpa - in aperta eccezione alla regola generale del nostro ordinamento di cui all'art. 2043 c.c., che fonda la responsabilità civile sulla colpa del danneggiante (per considerazioni analoghe v. Tribunale di Monza, Sez. Distaccata di Desio - caso "doctor glass", ord. 14 maggio 2001, dove si rileva

come, "anche volendo mascherare la responsabilità del provider sotto l'etichetta della culpa in vigilando, detta responsabilità sarebbe di fatto una responsabilità oggettiva legislativamente non tipizzata, non potendosi in alcun modo immaginare mezzi concreti attraverso i quali il provider potrebbe effettuare la propria vigilanza, considerato anche che il monitoraggio dovrebbe essere costante: è noto, infatti, che ogni sito è modificabile in qualsiasi momento, con una semplice operazione effettuabile anche "in remoto", 24 ore al giorno, 7 giorni su 7").
Di contro sembra certamente preferibile quella diversa ricostruzione che ritiene di fondare la responsabilità dell'Internet provider riferendosi all'art. 2043 ss. c.c. per quanto concerne i profili di responsabilità extracontrattuale e richiede di valutare ulteriormente i profili diacronici legati alla verificazione della lesione antigiuridica, interrogandosi se la diligenza esigibile imponga al provider l'adozione di misure volte a prevenire il compimento di illeciti da parte degli utenti o se invece gli imponga solo di eliminare gli effetti di tali illeciti, una volta che ne sia messo a conoscenza.
Sotto il primo profilo dell'affermazione di una diligenza preventiva, è stato così sostenuto che bisognerà distinguere tra il cd. access provider, il quale fornisce semplicemente l'accesso ad un canale di comunicazione, cd. Servizio di connettività, dal service provider, il quale, oltre a fornire un accesso alla rete, offra ai propri utenti un servizio di predisposizione, controllo o di monitoraggio delle informazioni e dati trasmessi sui loro servers. Ciò, in quanto, con riferimento al semplice access provider, mero fornitore di connettività, è da ritenere che l'obbligo di preventivo e incondizionato controllo sia del tutto estraneo alla tipologia di attività che le è propria, laddove diversamente si dovrebbe sostenere per il service\content provider, allorquando proprio la prestazione dallo stesso offerta abbia avuto ad oggetto un contributo, parziale o generale, alla realizzazione del sito e all'editing del materiale immesso in rete, sì da assumere pertanto delle funzioni editoriali o di direzione in senso lato (per tale distinzione elaborata dalla giurisprudenza statunitense, in materia di responsabilità del provider per violazione delle norme sul copyright v. Playboy Enterprises, Inc. v. Frena del 1993, Sega Entertainment, Ltd. v. Maphia del 1994, Religious Technology Center v. Netcom On-Line Communication Services del 1995; Sega Enterprises v. Sabella del 1995).
Seguendo tale modello ricostruttivo si perviene ad una conseguente, doverosa distinzione tra responsabilità preventiva e responsabilità successiva del provider, là dove la prima dovrebbe essere limitata ai service providers e sussisterebbe per il solo fatto di non aver impedito il verificarsi dell'illecito, mentre la seconda sarebbe invece attribuibile a qualsiasi provider (sia service che access), sussistendo per il fatto di non aver bloccato l'aggravamento dei danni conseguenti al comportamento antigiuridico.
Secondo un recente orientamento, a tal uopo, si è ritenuto che l'illecito che avviene su internet è da qualificare come un illecito permanente, essendovi una permanente ritrasmissione del dato, senza la possibilità del danneggiato d'impedirla, sicchè dovrebbe predicarsi sulla scorta dei principi civilistici, della normativa comunitaria e del codice di autoregolamentazione una regola di comportamento ed un modello di diligenza (obbligo di comunicare le generalità dell'utente che ha compiuto l'illecito, obbligo di attivarsi per rimuovere l'illecito) che fonda una posizione di garanzia del provider per tutto quanto accade successivamente alla scoperta del fatto da parte del provider.
Rispetto a tale posizione di garanzia risulterebbe configurabile la responsabilità dell'host provider per la violazione dell'obbligo di rimozione del dato illecito.
Conformemente a questo indirizzo interpretativo, si è espressa la giurisprudenza italiana più recente:
- con ordinanza del 27.06.97 poi confermata con la sentenza 19.10.1999 il Tribunale di Cuneo ha stabilito che il service provider non è responsabile della violazione dei diritti d'autore compiuta a mezzo di pagina web ospitata sul suo server, quando si sia limitato a concedere l'accesso alla rete;
- il già citato Tribunale di Roma ha deciso che il news server, cioè l'operatore che consente agli utenti di accedere ai news group, non è responsabile per i messaggi che attraversano i propri elaboratori in quanto si limita a mettere a disposizione lo spazio virtuale dell'area di discussione e non ha alcun potere di controllo e di vigilanza sugli interventi che vengono inseriti;
- analogamente Tribunale Bologna del 26 novembre 2001 ha ravvisato un'attività di fornitura di contenuti web nel provider che, pur limitandosi a fornire l'accesso al sito gestito (anche in piena autonomia) da altri, non consenta d'identificare il soggetto in questione né fornisca prova del contenuto degli accordi di utilizzazione dello spazio web con tale soggetto identificato, nel qual caso sembrerebbe essere stata affermata una responsabilità del provider per il solo fatto di avere garantito l'anonimato del gestore del sito, non consentendo ai terzi di conoscerne le generalità;
A fronte degli indirizzi giurisprudenziali su riferiti, peraltro, non mancano in dottrina ricostruzioni diverse che intendono discostarsi dal richiamo alla norma generale dell'art. 2043 c.c., volgendo, di contro, la propria attenzione ai regime speciali previsti dal c.c.: segnatamente secondo una diversa

isolata opzione ricostruttiva occorrerebbe fare riferimento all'art. 2050 c.c., affermandosi la possibilità di configurare una responsabilità oggettiva a carico del provider, siccome soggetto esercente un'attività pericolosa, con la conseguenza ulteriore che il gestore del sito, pertanto, dovrà rispondere del fatto illecito dell'utente del web, a meno che egli non provi "di aver adottato tutte le misure idonee ad evitare il danno".
La tesi non convince sia per l'intuitivo rilievo che, anzitutto, l'attività svolta dall'ISP non appare in sè oggettivamente e intrinsecamente fonte di pericolo (Tribunale Bologna, 26.11.2001), sia perché tutte le ipotesi di responsabilità oggettiva introdotte dal legislatore nazionale, in sede di recepimento di direttive comunitarie proprio tramite al ricorso all'art. 2050 c.c. (ex plurimis: cfr. art. 1 del d.p.R. 224/88 in materia di responsabilità da prodotto difettoso; art. 18 L.675/96, in materia di trattamento dei dati personali, art. 28 del d.p.R. 445/00, T.U. sulla documentazione amministrativa e firma digitale) sono comunque accomunate tutte dal fatto che esse presuppongono un effettivo potere di controllo sull'attività oggetto della tutela ed impongono, conseguentemente, l'adozione di misure di sicurezza adeguate, laddove tali operazioni di controllo, per come su rilevato, non sono "tecnicamente" possibili nei casi di specie.
Peraltro va rilevato come la materia della responsabilità dei vari tipi di providers è oggi offerta dal D. Lgs. 9 aprile 2003 n. 70, emanato in attuazione della direttiva 2000/31/CE, "relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico" (cd. "direttiva sull'e-commerce).
Segnatamente la questione della responsabilità degli ISP è affrontata negli articoli da 14 a 17, là dove si sono distinte e tipizzate le attività caratteristiche del prestatore di servizi in esame, individuandole nelle attività di "mere conduit", di "caching", di "hosting" e prevedendo conseguentemente per ciascuna di esse un regime differenziato di responsabilità.
L'art.14 del D.Lgs. 70/03 disciplina l'attività di "mere conduit", consistente nel trasmettere, su una rete di comunicazione, informazioni non proprie (cioè date dal destinatario del servizio) o nel fornire l'accesso alla Rete.
Per queste ipotesi l'articolo in commento stabilisce l'esonero da responsabilità per i prestatori, ritenendo e valorizzando correttamente la loro posizione di neutralità rispetto ai contenuti veicolati on line.
In tal modo si è stabilito che il carrier (cioè l'operatore telefonico) o l'access provider (ossia il fornitore di connettività) non sono responsabili di ciò che passa on line. Essi, peraltro, saranno ritenuti responsabili qualora o diano origine alla trasmissione (lett.a) o selezionino il destinatario della trasmissione (lett.b) ovvero, ancora, selezionino o modifichino le informazioni trasmesse.
Il successivo art. 15 è dedicato all'attività di memorizzazione temporanea, c.d. "caching" (si pensi alle attività di organizzazione delle mailing-list o di newsgroup). Come è noto, il caching ha lo scopo di aumentare la "capacità di portata" della Rete, conservando presso il server del prestatore, per un certo periodo, i dati cui hanno avuto accesso i fruitori del servizio, in modo da favorirne la consultazione in un secondo momento da parte di altri utenti. La norma prevede, a tal proposito, l'esenzione da responsabilità per il provider che, nella prestazione di un servizio della società dell'informazione, abbia effettuato "la memorizzazione automatica, intermedia e temporanea di tali informazioni, effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta".
L'esenzione da responsabilità, però, non potrà operare anche in tal caso qualora il provider modifichi le informazioni (lett.a), non si conformi alle condizioni di accesso alle informazioni (lett.b), non si conformi alle norme di aggiornamento delle informazioni, indicate in un modo ampiamente riconosciuto e utilizzato dalle imprese del settore (lett.c), interferisca con l'uso lecito di tecnologia ampiamente riconosciuta e utilizzata nel settore per ottenere dati sull'impiego delle informazioni (lett.d), non agisca prontamente per rimuovere le informazioni non appena venga a conoscenza del fatto che le informazioni sono state rimosse dal luogo dove si trovavano inizialmente sulla rete o che l'accesso alle informazioni è stato disabilitato oppure che un organo giurisdizionale o un'autorità amministrativa ne ha disposto la rimozione o la disabilitazione (lett.e).
In ultimo l'art. 16 disciplina l'attività di "hosting", cioè la attività del provider più diffusa nella rete e fondante la sua vis espansiva, che può andare dalla mera gestione del sito sul server, con memorizzazione delle pagine web, alla tenuta degli archivi informatici del cliente, con conservazione dei files di log, nel qual caso il prestatore (c.d."host provider") non è responsabile delle informazioni memorizzate a condizione che:
a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o circostanze che rendano manifesta l'illiceità dell'attività o dell'informazione;

b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso.
Il secondo comma poi esclude l'esenzione di responsabilità del provider – con conseguente sua piena responsabilità - se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore (è il caso, ad esempio, del content provider): in questa ipotesi, infatti, il provider non risulta estraneo alle informazioni veicolate, e quindi risponde – per fatto proprio – per gli eventuali contenuti illeciti immessi in Rete.
Ulteriore regola generale è poi quella che per i casi di "mere conduit", di "caching" e di "hosting" prevede la possibilità che il prestatore di servizi, anche ove non responsabile, sia tenuto – dietro provvedimento dell'autorità giudiziaria o amministrativa competente – ad impedire o a porre fine ad un illecito.
Con l'art. 17 del D.Lgs. 70/03 – vera e propria "norma di chiusura" del "sistema della responsabilità" dei providers – viene, infine, sancita l'assenza dell'obbligo generale di sorveglianza, affermandosi, al primo comma, che il prestatore dei servizi non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza né ad un obbligo di ricercare circostanze che indichino il compimento di atti illeciti. In tal modo il legislatore ha consacrato il su riferito riconoscimento della impossibilità tecnica per il provider di operare un controllo – preventivo o successivo – sulle informazioni memorizzate o trasmesse, escludendo così che possa operare un criterio di imputazione della responsabilità di carattere meramente oggettivo.
Il secondo comma dell'art. 17 impone poi al prestatore di informare prontamente l'autorità giudiziaria o quella amministrativa, qualora sia a conoscenza di presunte attività illecite riguardanti un proprio cliente (lett.a), ovvero di fornire, a richiesta delle autorità competenti, informazioni in suo possesso, al fine di permettere l'identificazione di un destinatario del servizio implicato in attività illecite (lett.b), per poi concludere al terzo comma nel senso della responsabilità del provider che, a fronte di richiesta dell'autorità giudiziaria o amministrativa, abbia ritardato la rimozione del materiale lesivo ovvero che, a conoscenza del carattere illecito del contenuto di un servizio da esso fornito, non abbia provveduto ad informarne l'autorità competente.
Tale essendo la disciplina, è stato acutamente osservato come essa si caratterizzi nel senso:
a) della irresponsabilità del provider che si limiti a fornire la connessione alla rete: in altri termini, l'access provider è equiparato al gestore di una rete telefonica il quale non può certamente essere tenuto responsabile per gli illeciti commessi dagli utenti della rete stessa;
b) della responsabilità del provider che non si limiti a fornire la connettività, ma eroghi servizi aggiuntivi, dal caching all'hosting (content provider), nel qual caso la responsabilità è generalmente subordinata alla circostanza che il provider sappia che l'attività o l'informazione trasmessa o svolta suo tramite siano illecite; tanto, seppure con la espressa limitazione derivante dalla circostanza che non si possa imporre al prestatore di servizi un obbligo generale di sorveglianza sulle informazioni trasmesse e memorizzate né, tanto meno, un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite;
c) della distinzione tra la posizione del provider e quella dell'editore o del direttore responsabile e ciò proprio al fine di sottrarlo all'applicazione delle più severe regole di responsabilità che in genere valgono per questi soggetti.
Il regime delineato, così come rileva la dottrina più recente, se, da un lato, conferma il ripudio, non solo di modelli di responsabilità oggettiva o per rischio di impresa, ma anche di modelli di responsabilità soggettiva aggravata, d'altro in positivo, si traduce nella subordinazione della responsabilità del provider alla circostanza che questi sappia della illiceità dell'attività o dell'informazione o anche, semplicemente, della esistenza dell'attività o dell'informazione.
La regola accolta è, dunque, quella in forza della quale il provider sarà responsabile dell'illecito posto in essere dall'utilizzatore allorché egli abbia piena consapevolezza del carattere antigiuridico dell'attività svolta da quest'ultimo.
La responsabilità del provider si configura, quindi, alla stregua di una responsabilità soggettiva: colposa, allorché il fornitore del servizio, consapevole della presenza sul sito di materiale sospetto, si astenga dall'accertarne l'illiceità e, al tempo stesso, dal rimuoverlo; dolosa, quando egli sia consapevole anche della antigiuridicità della condotta dell'utente e, ancora una volta, ometta di intervenire.
Tanto rilevato in punto di diritto, passando alla fattispecie in esame, va osservato come, nel merito, le difese della convenuta, sul presupposto esplicito e non contestato della sussistenza della violazione del diritto di autore del V. K. - perpetrato attraverso l'inserimento non autorizzato del suo scritto sul sito del comune di N. nel periodo di tempo compreso tra l'estate del 1998 e il gennaio 2001 -, si sono incentrate sulla circostanza che l'inserimento dello scritto in questione sul sito sarebbe stato voluto, ordinato e organizzato direttamente dal Comune, essendosi, di contro, limitata il servizio offerto dalla X.

L. alla fornitura del servizio di connettività e alla relativa gestione solo di natura tecnica del sito stesso sulla base di contenuti e materiali forniti dall'ente pubblico.
In altri termini con ogni evidenza la convenuta assume di essere un fornitore di mero service provider con le conseguenze in punto di diritto su esaminate.
Ora, sulla base della normativa su richiamata, non vi può essere dubbio alcuno che, una volta allegato e provato il fatto illecito dedotto dal V. K. in ordine alla violazione del diritto d'autore sulla propria opera storiografica, l'eccezione, avente ad oggetto la natura specifica della tipologia particolare di servizio offerto dalla convenuta al Comune di N. - sulla scorta di una deliberazione comunale che, peraltro, nessuna delle parti in giudizio ha prodotto e che entrambe hanno dato come pacificamente esistente, senza peritarsi di provarne i contenuti –, doveva, in virtù dell'onere probatorio ex art. 2697 c.c., essere positivamente dimostrata dalla medesima convenuta o per testi ovvero producendo idonea e conducente documentazione, la quale attestasse l'invio da parte del Comune di N. degli atti, dei materiali e delle fotografie poi inserite nel sito dalla stessa gestito. Così da rendere conclamata la sua funzione mera di fornitore di servizi di sola connettività telematica.
Tale prova non è stata in alcun modo fornita dalla X. L., che, anzi, proprio dalla documentazione in atti risulta che con missiva del Comune di N. del 19.2.2001, n. prot. 4869, il Comune in questione espressamente negava di avere "mai autorizzato e\o obbligato la ditta X. L. a riprodurre anche parzialmente opere coperte dal diritto di copyright da parte di terzi ed ad avvalersi e\o copiare pedissequamente determinate opere in special modo quella contestata", nonché significativamente precisava che "laddove la società Cormorano l'ha ritenuto necessario, ha chiesto e ottenuto dal Comune l'autorizzazione alla pubblicazione di pagine inerenti il tetto ligneo della cattedrale".
A riprova proprio il Comune allegava alla detta missiva una copia fotostatica di una pagina del sito in questione relativa al tetto ligneo della cattedrale di N., pagina nella quale, diversamente da quanto avvenuto nel caso di specie, si rendeva noto espressamente che "il testo è tratto da scritti del prof. Giovanni De Francesco. Le foto di Pippo Nicolosi sono tratte, su autorizzazione dell'Amministrazione comunale di N. dal CD creato da Media Tres Multimedia Catania".
A fronte di tale decisiva prova documentale, nulla di speculare è stato allegato e provato dalla convenuta, la quale allora deve, quale proprietaria del dominio presso il quale veniva gestito e pubblicato il sito in esame, ritenersi responsabile dei materiali e dei scritti nello stesso inseriti secondo il regime di responsabilità che caratterizza il content provider, al quale incombe l'obbligo previo di controllare e verificare ogni eventuale profilo di lesività dei contenuti resi ostensibili nel sito dallo stesso creato, organizzato e gestito. Né a diversa soluzione sembra potersi giungere in dipendenza della dedotta natura gratuita del servizio reso, trattandosi nel caso di specie di illecito extracontrattuale rilevante ai sensi dell'art. 2043 ss. c.c..
Ritenuta quindi sussistente una fattispecie di responsabilità extracontrattuale per violazione del diritto di autore, venendo alla concreta determinazione del quantum risarcibile a titolo di danno economico subito dal suo autore, va rilevato come nessun concreto elemento sia stato allegato e prodotto dall'attore, il quale sul punto non ha ritenuto opportuno neanche richiedere una consulenza tecnica d'ufficio ai fini della quantificazione dei danni economici subiti con la relativa allegazione di parametri oggettivi di quantificazione del danno.
Le spese seguono la soccombenza ex art. 91 c.p.c..

P.Q.M.

Il Giudice, definitivamente pronunciando nella causa civile iscritta al n. 5464\01 R.G., ogni ulteriore domanda disattesa,
a) Dichiara l'illegittimità del comportamento posto in essere dalla società convenuta in violazione del diritto di autore di V. K. sull'opera storiografica di cui in motivazione;
b) Inibisce alla cooperativa X. L. a r.l. di utilizzare per il futuro l'opera storiografica dell'attore;
c) Rigetta la domanda di risarcimento del danno proposta da V. K. nei confronti della società convenuta;
d) condanna la cooperativa X. L. a r.l. al rimborso in favore dell'attore delle spese legali che liquida in Euro E. 2000, di cui E. 150, 00 per spese, E. 850, 00 per diritti di procuratore e E. 1000, 00 per onorari di avvocato, oltre iva e c.p.a. come per legge.
Così deciso in Catania il 25.6.2004
Il Giudice
dott. Mariano Sciacca

L'invio non richiesto di messaggi pubblicitari via internet (spamming) cagiona al destinatario un pregiudizio di ordine patrimoniale e morale risarcibile ai sensi dell'articolo 2043 del codice civile.

NUMERO SCHEDA: 5004

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

FONTE: ITALIA OGGI

DATA: 23/06/2004

PAGINA: 26

RIFERIMENTO NORMATIVO: art. 2043 c.c.

NATURA ATTO: SENTENZA

DATA ATTO: 10/06/

ORGANO: GIUDICE DI PACE

La sentenza, qui di seguito allegata in forma integrale, affronta la problematica relativa all'invio di messaggi pubblicitari via internet nel caso in cui il ricevente non abbia dato il proprio consenso all'invio degli stessi.
Tale invio non autorizzato oltre a ledere i principi contenuti nella normativa sulla privacy cagiona un danno patrimoniale e morale al detentore dell'indirizzo di posta elettronica che è obbligato da un lato, a sostenere i costi di collegamento alla rete per la lettura dei messaggi inviati, dall'altro è costretto a perdere diverso tempo nel selezionare i messaggi arrivati. Pertanto sulla base della *vis* espansiva dell'articolo 2043 il giudice di pace di Napoli ha condannato la società al risarcimento del danno - morale e patrimoniale- lamentato dall'attore.
Inoltre, il giudice di pace di Napoli condanna la società convenuta all'immediata cancellazione dei dati relativi all'attore e alla pubblicazione su vari quotidiani del dispositivo della sentenza.

Si allega il testo integrale della sentenza.

Giudice di pace di Napoli – Sezione prima – sentenza 7-10 giugno 2004
Giudice: Contrada

Ricorrente: Pisani

Svolgimento del processo

Con atto di citazione notificato il 12 novembre 2003 alla srl Nencini Sport, l'attore avvocato Angelo Pisani, premesso di essere titolare di una casella e di un indirizzo di posta elettronica personale e riservato, attraverso cui, abitualmente riceve via e-mail notizie, comunicazioni ed altre informazioni di carattere personale e professionale, utili per la sua attività, premesso che esso avvocato Angelo Pisani il 3 settembre 2003 aveva nella sua casella di posta elettronica un messaggio pubblicitario inviato dalla srl Nencini Sport che, a grandi caratteri, illegittimamente ed arbitrariamente proponeva l'acquisto di numerosi articoli sportivi, conveniva pertanto in giudizio la srl Nencini Sport per l'udienza del 15

dicembre 2003 per sentirla condannare al risarcimento dei danni materiali e morali per responsabilità extracontrattuale da fatto illecito, per danni alla vita di relazione ed esistenziali nella misura di euro 1032.91, previa dichiarazione di responsabilità per illecito trattamento tramite internet dei dati dell'attore da parte della srl Nencini Sport, oltre interessi legali dalla domanda e rivalsa di spese, con obbligo immediato alla cancellazione e rimozione dei propri dati dalla banca dati informatica pubblicitaria Nencini Sport e con autorizzazione alla pubblicazione della emananda sentenza su cinque quotidiani e due settimanali di interesse nazionale. Instaurato il giudizio la convenuta società srl Nencini Sport non si costituiva per cui ne va dichiarata la contumacia. Esibita copiosa documentazione e dopo l'udienza di trattazione la causa veniva rinviata per la precisazione delle conclusioni e quindi passava in decisione.

Motivi della decisione

La giurisprudenza recente accredita sempre più la tesi che il sistema degli articoli 2043 e ss. Cc è atipico e aperto, nel senso che non prefigura a priori precise e chiuse categorie di illeciti, non offre criteri circostanziati di applicazione della clausola generale della ingiustizia del danno. Per cui questo giudizio nella fattispecie ritiene applicabile l'articolo 2043 Cc, infatti a prescindere dal fatto che gli indirizzi di posta elettronica recano dati di carattere p personale da trattare nel rispetto dell'articolo 1, comma 1, lettera c) della legge 675/96 e cioè la loro utilizzazione per scopi promozionali e pubblicitari è possibile solo se il soggetto cui si riferiscono abbia manifestato in precedenza un consenso libero, specifico e informato come stabilito dalla direttiva Ce 2002/58 e dalla decisione 11 gennaio 2001 del Garante della privacy. Infatti l'utilizzo della posta elettronica comporta una lesione ingiustificata dei diritti dei destinatari, costretti ad impiegare diverso tempo per mantenere un collegamento e per ricevere, come pur per esaminare e selezionare, tra i diversi messaggi ricevuti, quelli attesi o ricevibili, nonché a sostenere i relativi costi per il collegamento telefonico (incrementati anche da messaggi di dimensioni rilevanti che rallentano tali operazioni). Ma a prescindere dalla indubitabile responsabilità della srl Nencini Sport conseguente ad un comportamento illecito dei suoi dipendenti, l'esigenza di risarcire il danno nel modo più agevole ed ampio possibile ha indotto la giurisprudenza ad innovare le tendenze della tradizione e ad estendere in via generale le regole di responsabilità oggettiva o per rischio che prima erano confinate ad ipotesi di eccezioni e si è affermata una interpretazione teleologica delle norme sulla base della quale l'articolo 2043 Cc assolve la funzione di regola generale di responsabilità accanto ad una serie di altre regole relative ad ipotesi particolari di attività fondate su diversi criteri di imputazioni. Pertanto si è addirittura superato il pregiudizio di una volta di nessuna responsabilità senza colpa ed è corrente l'opinione che in materia di responsabilità extracontrattuale siano risarcibili anche i danni non previsti. Pertanto l'invio di posta elettronica indesiderata nella fattispecie è illegittima sotto due profili: da un lato per la scorrettezza e illiceità del trattamento dei dati personali dell'attore da parte della convenuta e dall'altro lato provoca una illegittima intrusione e invasione nella sua sfera di riservatezza come stabilito dal Garante della privacy (gli indirizzi di posta elettronica non sono utilizzabili da chiunque in quanto non si tratta di dati pubblici alla stregua degli elenchi telefonici tradizionali). La domanda dell'attore risulta fondata sia per l'*an* che per il *quantum debeatur* e va accolta per quanto di ragione: la versione fornita dall'attore trova pieno riscontro nella documentazione esibita e nelle risultanze istruttorie. Infatti avendo l'attore fornito la prova del proprio assunto, incombeva sulla parte convenuta l'onere di provare l'esistenza di fatti modificativi ed estintivi del diritto dell'attore. Tanto premesso deve dichiararsi la convenuta srl Nencini Sport responsabile per fatto illecito *ex* articolo 2043 Cc essendo chiaro e definito il nesso di causalità tra l'evento ed il danno ingiusto subito dall'attore. Tenuto conto del fatto che l'attore ha fornito prova del danno materiale e morale derivatogli dall'illecito trattamento dei propri dati e dall'invio illegittimo da parte della società convenuta in data 3 settembre 2003 di un messaggio pubblicitario a grandi caratteri che proponeva l'acquisto di numerosi articoli sportivi nella casella di posta elettronica (angelopisani@tin.it) utilizzato a scopi personali e professionali per l'attività di avvocato, tenuto conto del danno alla vita di relazione del danno esistenziale conseguente alla lesione e al turbamento della qualità di vita dell'attore, tenuto conto della documentazione esibita e delle risultanze istruttorie, la società convenuta srl Nencini Sport va condannata al risarcimento dei danni materiali e morali nella misura di euro 1000 determinata in via equitativa sia per il danno patrimoniale che per il danno morale, tenuto conto delle spese generali e degli inconvenienti e perdite di tempo subite, derivante dall'illecito invio di corrispondenza elettronica a scopo pubblicitario non effettuato sulla base del consenso preventivo ed informato dell'attore, oltre interessi legali dalla domanda. Le spese processuali seguono la soccombenza e vanno poste a carico

della convenuta, tenuto conto della natura e del valore della causa e dell'attività professionale svolta.

PQM

Il GdP di Napoli, in accoglimento della domanda attorea, dichiara la convenuta srl Nencini Sport obbligata previa cancellazione e rimozione dei dati dell'attore dalla banca dati della srl Nencini Sport all'immediato invio di certificazione di tutto quanto gestito e trattato tramite i dati personali dell'attore e la immediata consegna all'attore di dichiarazione liberatoria circa la cancellazione ed eliminazione dei dati dell'attore dalla sua banca dati, condanna la convenuta srl Nencini Sport a pagare all'attore avvocato Angelo Pisani la complessiva somma di euro 1000 oltre interessi legali dalla domanda, e le spese di causa che liquida in euro 750 (di cui euro 100 per spese e il resto per diritti ed onorario) oltre Iva, Cpa e quota spese generali nella misura di legge, autorizzando l'attore alla pubblicazione del dispositivo della emanando sentenza sui quotidiani il "Corriere della Sera", "La Repubblica", "Il Giornale" e "Il Messaggero", nonché sui settimanali "Panorama" e "L'Espresso".

Iniziano i lavori della commissione ministeriale sull'antipirateria digitale in attuazione della legge Urbani 128/2004, entrata in vigore dopo la pubblicazione sulla G.U. n. 119 del 22/05/2004.

NUMERO SCHEDA: 4812

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

FONTE: ITALIA OGGI

AUTORE: Antonio CICCIA

DATA: 25/05/2004

PAGINA: 26

RIFERIMENTO NORMATIVO: legge Urbani 128/2004

NATURA ATTO: COMMENTO

DATA ATTO: 24/05/2004

Il ministro dell'innovazione tecnologica, Lucio Stanca, ha dichiarato che in data 24 maggio 2004 sono stati avviati i lavori della commissione interministeriale per lo sviluppo del mercato dell'industria dei prodotti intellettuali digitali e per l'adeguamento della legge 128/2004 (la c.d. legge Urbani, che ha convertito il d.l. 72/2004), entrata in vigore dopo la pubblicazione sulla Gazzetta Ufficiale n. 119 del 22/05/2004. Ai lavori parteciperanno i rappresentanti degli operatori e delle imprese di settore delle associazioni rappresentative degli autori e dei consumatori, e delle pubbliche amministrazioni centrali e locali. Il compito della commissione è di rafforzare le norme contro la pirateria informatica mettendo allo studio iniziative di contrasto da affiancare agli strumenti normativi vigenti, per impedire l'uso illecito delle cosiddette "copie pirata".

L'obiettivo della legge è quello di introdurre la tutela del diritto d'autore in internet con le seguenti modalità:

- se si immettono opere in rete è obbligatorio l'avviso con l'indicazione che sono stati assolti gli obblighi derivanti dal diritto d'autore e dai diritti connessi;
- si deve dare avviso anche delle sanzioni previste dalla legge per chi viola il diritto d'autore;
- entrambi gli avvisi devono essere adeguatamente visibili;
- le disposizioni di attuazione saranno emanate tramite decreto, preceduta da accordi tra Siae e associazioni delle categorie interessate;
- si inserisce una nuova fattispecie di reato con una integrazione all'art. 171 ter della legge sul diritto d'autore, in pratica si aggiunge la lettera a-bis) al comma secondo del citato articolo, che dispone la reclusione da uno a quattro anni e con la multa fino a € 15.493, chiunque per trarne profitto, comunica al pubblico immettendola in un sistema di reti telematiche mediante connessioni di qualsiasi genere, un'opera protetta o parte di essa.;
- il dolo di lucro previsto dall'art. 171 ter primo comma diviene dolo di profitto ;
- i provider devono comunicare alle autorità di polizia le informazioni in proprio possesso utili alla individuazione dei gestori dei siti e degli autori delle condotte illecite.

Il Governo incrementa la lotta ai virus informatici con la creazione di un centro nazionale per la sicurezza informatica (Cnsi).

NUMERO SCHEDA: 4600

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

FONTE: ITALIA OGGI

AUTORE: Stefano SANSONETTI

DATA: 21/04/2004

Quello dei virus informatici è un problema che l'anno scorso ha investito almeno il 40% della pubblica amministrazione. Il Governo ha così deciso depotenziare la lotta contro l'intrusione dei virus le cui fonti si annidano prevalentemente in brasile e nel Sudest asiatico, attraverso la creazione di una nuova Agenzia denominata centro nazionale per la sicurezza informatica (Cnsi) che gestirà un nuovo sistema di governo della sicurezza Ict nella pubblica amministrazione. Tutto questo all'interno di un progetto che ai primi di maggio vedrà la nascita di un primo e nuovo organismo denominato Govcert.it il cui compito sarà quello di monitorare la rete, intercettare i tentativi di intrusione e prevenire le mosse dei pirata informatici. Per questo progetto il Governo ha stanziato cinque milioni di euro.

Per notizie più dettagliate sulle problematche del cyberterrorismo e sugli strumenti messi a punto dal governo italiano per fronteggiare tale problema sono consultabili sul sito internet www.governo.it .

Si allega il testo del decreto interministeriale del 24 luglio 2002

Decreto interministeriale 24 luglio 2002

Istituzione del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni

ART. 1
Istituzione del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni
1. E' istituito il Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni (di seguito denominato Comitato) con funzioni di indirizzo e coordinamento delle iniziative in materia di sicurezza nelle tecnologie dell'informazione e della comunicazione nelle pubbliche amministrazioni, di cui alla direttiva del Ministro per l'innovazione e le tecnologie del 16 gennaio 2002.
2. Il Comitato è composto da cinque esperti, dotati di comprovata e qualificata competenza professionale in materia, di cui uno con funzioni di Presidente.

3. Il Presidente e uno dei membri del Comitato sono nominati dal Ministro delle comunicazioni. I restanti tre membri sono nominati dal Ministro per l'innovazione e le tecnologie.
4. Il Comitato è così composto:
Presidente:
Pref. Vittorio Stelo (Segretario Generale del Ministero delle comunicazioni), nominato dal Ministro delle comunicazioni;
Membri:
- Avv. Massimo Condemi (Capo della Segreteria Tecnica del Ministro delle comunicazioni), nominato dal Ministro delle comunicazioni;
- Avv. Carlo Sarzana di S. Ippolito (Presidente aggiunto onorario della Corte di cassazione), nominato dal Ministro per l'innovazione e le tecnologie;
- Prof. Danilo Bruschi (Università degli studi di Milano Dipartimento di scienze dell'informazione), nominato dal Ministro per l'innovazione e le tecnologie;
- Dott. Giorgio Tonelli (Senior Partner Ambrosetti), nominato dal Ministro
per l'innovazione e le tecnologie.
5. Il Comitato, nell'assolvimento dei propri compiti, opera sulla base degli indirizzi strategici definiti, nell'ambito delle rispettive competenze istituzionali, dal Ministro delle comunicazioni e dal Ministro per l'innovazione e le tecnologie.
6. Per lo svolgimento dei propri compiti, il Comitato si avvale del Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio e dell'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (ISCTI) e del Gruppo di lavoro per la sicurezza delle reti e la tutela delle comunicazioni operante presso il Ministero delle comunicazioni. Si avvale, altresì, di qualificate risorse esterne all'amministrazione provenienti dalla comunità scientifica, dalle imprese industriali e dai servizi, esperte in problemi della sicurezza informatica e delle comunicazioni.
7. Il Comitato termina i suoi lavori entro il 31 dicembre 2004. E' fatto salvo l'eventuale rinnovo del Comitato.
ART. 2
Funzioni del Comitato
1. Il Comitato, al fine del raggiungimento di un livello di sicurezza nelle informazioni conforme a criteri standard internazionali e per garantire integrità e affidabilità dell'informazione, formula le proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la pubblica amministrazione, in particolare ai fini della redazione:
a) del Piano nazionale della sicurezza delle tecnologie dell'informazione e comunicazione della pubblica amministrazione, di cui verifica annualmente lo stato di avanzamento, identificando le eventuali misure correttive;
b) della predisposizione del modello organizzativo nazionale di sicurezza ICT per la pubblica amministrazione, del quale verifica la relativa attivazione e applicazione.

2. Il Comitato formula, inoltre, proposte in materia di regolamentazione della certificazione e valutazione della sicurezza, nonché ai fini della predisposizione di criteri di certificazione e delle linee guida per la certificazione di sicurezza ICT per la pubblica amministrazione, sulla base delle normative nazionali, comunitarie e internazionali di riferimento.
3. Il Comitato elabora linee guida per la predisposizione delle intese con il Dipartimento della funzione pubblica in ordine alla formazione dei dipendenti pubblici in tema di sicurezza ICT.
ART. 3
Poteri del Comitato
1. Il Comitato può, per le finalità di cui all'articolo 1:
a) convocare e procedere ad audizioni di rappresentanti dei produttori di apparecchiature e di sistemi informatici e telematici, degli organismi di telecomunicazioni e di qualsiasi altro soggetto dotato di specifiche competenze nelle materie di interesse del Comitato;
b) richiedere documentazione tecnica ed amministrativa presso i costruttori di apparecchiature e di sistemi informatici e telematici, nonché presso gli organismi di telecomunicazioni;
c) richiedere l'accesso, anche per mezzo di organi tecnici delle amministrazioni interessate o ad esse collegati, agli impianti, ai locali ed ai centri elaborazione dati degli organismi di telecomunicazioni e dei produttori di sistemi informatici e telematici.
2. Ogni quattro mesi il Comitato, tramite il suo Presidente, riferisce sulle iniziative adottate e sul relativo stato di avanzamento al Ministro delle comunicazioni e al Ministro per l'innovazione e le tecnologie, i quali possono chiedere in ogni momento informazioni sull'andamento dei lavori del Comitato.
ART. 4
Organizzazione del Comitato
1. Il Comitato ha sede presso il Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio e si avvale di una segreteria tecnica, con compiti di supporto tecnico e per la raccolta, la selezione e l'elaborazione del materiale rilevante ai fini dell'attività del Comitato stesso.
2. Il Ministero delle comunicazioni e il Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio pongono a disposizione del Comitato il personale occorrente per lo svolgimento dei compiti di segreteria tecnica..
ART. 5
Profili finanziari
1. Ai componenti del Comitato non spettano compensi in relazione all'incarico conferito con il presente decreto, salvo il rimborso, per i componenti non residenti a Roma, delle eventuali spese di viaggio e di soggiorno sostenute per gli spostamenti connessi allo svolgimento dell'attività del Comitato.
2. Alla spesa occorrente a norma del comma 1 si fa fronte, per i membri del Comitato nominati dal Ministro per l'innovazione e le tecnologie, utilizzando le disponibilità dei fondi iscritti sul capitolo n. 660 del centro di responsabilità "Innovazione e tecnologie" del bilancio della Presidenza del Consiglio dei ministri, e, per i membri nominati dal Ministro delle comunicazioni, utilizzando le disponibilità dei fondi iscritti sui capitoli n. 1005 e 1372 dello stato di previsione della spesa del Ministero delle comunicazioni, nonché sui corrispondenti capitoli per gli esercizi successivi.

Provvedimento del Garante per la protezione dei dati personali contro lo spamming

NUMERO SCHEDA: 3750

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

FONTE: WWW.GARANTEPRIVACY.IT/GARANTE/NAVIG/JSP/INDEX.JSP

DATA: 03/09/2003

NATURA ATTO: ATTI

DATA ATTO: 03/09/2003

Il Garante per la protezione dei dati personali ha adottato un nuovo provvedimento per precisare vari aspetti legati all'invio in Internet di e-mail promozionali o pubblicitarie, anche alla luce del recepimento della recente direttiva europea avvenuto con il Codice in materia di protezione dei dati personali (decreto legislativo n. 196/2003).

Il Garante ha posto in rilievo i profili penali del fenomeno dello *spamming* (invio massiccio ed indiscriminato di messaggi pubblicitari non richiesti) che interessa singoli utenti internet e piccole e medie imprese costrette a sopportare vari costi.

La normativa sulla privacy non permette di utilizzare indirizzi di posta elettronica per inviare messaggi indesiderati a scopo promozionale o pubblicitario anche quando si omette di indicare in modo chiaro il mittente del messaggio e l'indirizzo fisico presso il quale i destinatari possono rivolgersi per chiedere che i propri dati personali non vengano più usati.

Inviare e-mail pubblicitarie senza il consenso del destinatario è vietato dalla legge. Se questa attività, specie se sistematica, è effettuata a fini di profitto si viola anche una norma penale e il fatto può essere denunciato all'autorità giudiziaria. Sono previste varie sanzioni e, nei casi più gravi, la reclusione.

Si allega il testo del provvedimento

PREMESSO:

1. I DISAGI DI NUMEROSI UTENTI

Continuano a pervenire a questa Autorità diverse centinaia di reclami e segnalazioni da parte di utenti di reti telematiche e di associazioni per la tutela dei diritti di utenti e consumatori, che contestano la ricezione di messaggi di posta elettronica per scopi promozionali, pubblicitari, di informazione commerciale o di vendita diretta, inviati senza che gli interessati abbiano manifestato in precedenza il proprio consenso informato.

Numerosi interessati espongono anche ulteriori disagi derivanti dalla costante ripetizione di analoghi messaggi da parte di uno stesso mittente titolare del trattamento, dai vani tentativi esperiti per ottenere sia la cancellazione del proprio indirizzo di posta elettronica presso i mittenti, sia l'interruzione di altri messaggi. Altre segnalazioni riguardano gli inconvenienti che derivano dalla ricezione di e-mail anonime o prive dell'indicazione di un indirizzo, oppure delle coordinate veritiere di un reale mittente.

Nella prevalenza dei casi, agli interessati non è stato previamente richiesto, come dovuto, uno specifico consenso preceduto da un'idonea informativa che illustri adeguatamente le modalità e le caratteristiche dei messaggi.

In altri casi i messaggi sono inviati da imprese -anche in questo caso senza consenso- per promuovere, presso clienti, prodotti o servizi analoghi a quelli forniti in un rapporto contrattuale, oppure per offrire altri tipi di prodotti o servizi distribuiti anche da terzi.

Il Garante ha fornito assistenza a numerosi cittadini, indicando le opportune modalità di tutela; ha poi attivamente cooperato in sede comunitaria per l'adozione di decisioni comuni alle autorità di garanzia dei Paesi dell'Unione europea, pubblicate nel sito Internet di quest'ultima e in quello del Garante (www.garanteprivacy.it).

L'Autorità ha anche accolto numerosi ricorsi (art. 29 legge n. 675/1996), a seguito dei quali sono stati impartiti specifici divieti di trattamento dei dati. Sono stati altresì avviati i procedimenti per applicare le pertinenti sanzioni amministrative e sono stati trasmessi gli atti all'autorità giudiziaria penale nei casi in cui erano configurabili reati.

Con la collaborazione di forze di polizia, incaricate da questa Autorità di svolgere i necessari controlli e di dare esecuzione ai provvedimenti, sono stati eseguiti in loco, presso fornitori di servizi ed altri titolari

di trattamento, vari provvedimenti di sospensione temporanea di ogni operazione illecita del trattamento dei dati personali da parte di società risultate responsabili di attività svolte in modo sistematico. Infine, sono stati eseguiti accertamenti presso altri fornitori di servizi di accesso ad Internet o ulteriori soggetti, per verificare la rispondenza dei trattamenti di dati alla normativa vigente.
A conclusione di queste attività, il Garante ravvisa la necessità di adottare un provvedimento di carattere generale per indicare le misure che gli operatori del settore devono adottare al fine di conformarsi alla disciplina generale sull'uso dei dati personali, specie nel settore delle comunicazioni (in particolare, alla legge 31 dicembre 1996, n. 675, al decreto legislativo 13 maggio 1998, n. 171 e al decreto legislativo 22 maggio 1999, n. 185). L'Autorità ritiene inoltre necessario inibire il trattamento illecito di dati risultante da altre segnalazioni il cui esame è stato riunito in un unico procedimento, in particolare di quelle relative a titolari di trattamento identificabili.

2. INVIO LECITO DI POSTA ELETTRONICA PUBBLICITARIA

Gli indirizzi di posta elettronica recano dati di carattere personale da trattare nel rispetto della normativa in materia (art. 1, comma 1 lett. c), legge n. 675).
La loro utilizzazione per scopi promozionali e pubblicitari è possibile solo se il soggetto cui riferiscono i dati ha manifestato in precedenza un consenso libero, specifico e informato.
Il consenso è necessario anche quando gli indirizzi sono formati ed utilizzati automaticamente con un software senza l'intervento di un operatore, o in mancanza di una previa verifica della loro attuale attivazione o dell'identità del destinatario del messaggio, e anche quando gli indirizzi non sono registrati dopo l'invio dei messaggi. Questo assetto, basato su una scelta dell'interessato c.d. di opt-in, è stato ribadito nel 1998 (con il d.lg. n. 171) prima ancora che una recente direttiva comunitaria lo estendesse a tutti i Paesi dell'Unione europea (n. 2002/58/CE in fase di recepimento in Italia, pubblicata sulla G.U.C.E. n. L 201 del 31 luglio 2002).
Questa Autorità si è pronunciata più volte in materia ribadendo che la circostanza che gli indirizzi di posta elettronica possano essere reperiti con una certa facilità in Internet non comporta il diritto di utilizzarli liberamente per inviare messaggi pubblicitari (cfr., ra l'altro, la decisione dell'11 gennaio 2001 - in Bollettino del Garante n. 16).
In particolare, i dati dei singoli utenti che prendono parte a gruppi di discussione in Internet sono resi conoscibili in rete per le sole finalità di partecipazione ad una determinata discussione e non possono essere utilizzati per fini diversi qualora manchi un consenso specifico (art. 9, comma 1, lettere a) e b), legge n. 675).
Ad analoga conclusione deve pervenirsi per gli indirizzi di posta elettronica compresi nella lista "anagrafica" degli abbonati ad un Internet provider (qualora manchi, anche in questo caso, un consenso libero e specifico), oppure pubblicati su siti web di soggetti pubblici per fini istituzionali.
Tali considerazioni valgono anche con riferimento ai messaggi pubblicitari inviati a gestori di siti web - anche di soggetti privati- utilizzando gli indirizzi pubblicati sugli stessi siti, o che sono reperibili consultando gli elenchi dei soggetti che hanno registrato i nomi a dominio. In quest'ultimo caso, infatti, la conoscibilità in rete degli indirizzi è volta a identificare il soggetto che è o appare responsabile, sul piano tecnico o amministrativo, di un nome a dominio o di altre funzioni rispetto a servizi Internet (per la tutela di vari diritti sul piano civile e penale, anche ai sensi della legge n. 675) e non anche a rendere l'interessato disponibile all'invio di messaggi pubblicitari).
In tutti questi casi, l'utilizzo spesso massivo della posta elettronica comporta una lesione ingiustificata dei diritti dei destinatari, costretti ad impiegare diverso tempo per mantenere un collegamento e per ricevere, come pure per esaminare e selezionare, tra i diversi messaggi ricevuti, quelli attesi o ricevibili, nonché a sostenere i correlativi costi per il collegamento telefonico (incrementati anche da messaggi di dimensioni rilevanti che rallentano tali operazioni), oppure ad adottare "filtri", a verificare più attentamente la presenza di virus, o a cancellare rapidamente materiali inadatti a minori specie in ambito domestico.
Il fenomeno interessa anche piccole e grandi imprese destinatarie di un elevato numero di messaggi, le quali devono farsi carico di misure interne e di costi anche organizzativi per contrastarlo.
Questo ingiustificato riversamento sugli utenti dei costi pubblicitari si verifica anche relativamente a messaggi inviati da singole persone fisiche che, in vari casi esaminati, non si limitano ad una comunicazione episodica, ma intraprendono una comunicazione sistematica per fini personali o, addirittura, una diffusione di dati cui è applicabile la disciplina in materia di protezione dei dati personali (art. 3 legge n. 675).

3. IL QUADRO GIURIDICO SU INFORMATIVA E CONSENSO

La legge individua il contenuto dell'informativa agli interessati, nonché i casi in cui è necessario il consenso espresso dell'interessato o è possibile prescinderne (artt. 10, 11, 12 e 20 legge n. 675).

Al riguardo va nuovamente rilevato che non può farsi a meno del consenso ritenendo che i dati personali relativi all'indirizzo di posta elettronica -e all'indirizzo in particolare- siano "pubblici" in quanto conoscibili da chiunque.
Le disposizioni normative che si riferiscono a questo aspetto (artt. 12, comma 1, lett. c) e 20, comma 1, lett. b) legge cit.) sono infatti applicabili solo quando vi è un pubblico registro, elenco, atto o documento conoscibile da chiunque perché vi è una specifica disciplina che ne impone la conoscibilità indifferenziata da parte del pubblico, e non anche quando i dati personali sono conoscibili da chiunque per mere circostanze di fatto (si pensi, oltre ai casi già richiamati di raccolta su siti web o di messaggi trasmessi su newsgroup o su mailing list, agli indirizzi di posta elettronica raccolti in rete tramite appositi software o mediante comuni motori di ricerca).
Il principio del consenso è quindi già operante nel nostro ordinamento prima ancora di essere affermato senza eccezioni su scala europea, dalla menzionata direttiva n. 2002/58 in fase di recepimento, a tutta la posta elettronica comunque inviata per fini di commercializzazione diretta (si vedano in particolare l'art. 13 e il considerando n. 40).
Il quadro evidenziato trova conferma nella disciplina sulla protezione dei consumatori nei contratti a distanza che, in riferimento al rapporto sottostante ai fini del quale si procede al trattamento di dati personali, vieta ai fornitori l'impiego della posta elettronica in mancanza del consenso preventivo del consumatore, in relazione a determinati scopi tra i quali rientrano anche quelli pubblicitari (art. 10, comma 1, d.lg. 22 maggio 1999, n. 185).
Per gli aspetti relativi alla protezione dei dati personali non devono essere peraltro considerate le disposizioni del recente decreto legislativo 9 aprile 2003, n. 70, sul commercio elettronico, dichiarate in proposito espressamente inapplicabili (art. 1, comma 2, lett. b) d.lg. n. 70 cit.).
Il consenso, da documentare per iscritto, deve essere manifestato liberamente, in modo esplicito e in forma differenziata rispetto alle diverse finalità e alle categorie di servizi e prodotti offerti, prima dell'inoltro dei messaggi (art. 11 legge n. 675).
Tale disciplina non può essere elusa inviando una prima e-mail che, nel chiedere un consenso abbia comunque un contenuto promozionale oppure pubblicitario, oppure riconoscendo solo un diritto di tipo c.d. "opt-out" al fine di non ricevere più messaggi dello tesso tenore.
Al contrario, è opportuna e va incoraggiata la prassi di alcuni fornitori i quali, dopo aver ottenuto realmente un valido consenso dei destinatari, danno semplice conferma della sua manifestazione, attraverso un messaggio volto unicamente ad annunciare il successivo inoltro di materiale pubblicitario. Tale prassi, se utilizzata correttamente, consente tra l'altro di verificare l'effettiva corrispondenza dell'indirizzo di posta elettronica ai soggetti che avevano espresso il consenso, nonché di accertare il permanere di tale volontà.
L'insieme dei diritti riconosciuti dalla legge agli utenti determina, in caso di loro violazione, un trattamento illecito dei dati che:
- è già vietato direttamente dalla legge, senza che sia necessario adottare uno specifico provvedimento interdittivo del Garante dell'autorità giudiziaria;- determina, a seconda dei casi, l'applicazione di sanzioni amministrative pecuniarie, in particolare per · omessa informativa od omessa notificazione (artt. 10, 34 e 39 legge n. 675; art. 12 d.lg. n. 185/1999);
- comporta il rimborso delle spese e dei diritti relativi al procedimento attivato da un fondato ricorso al Garante, oppure da un'azione dinanzi al giudice civile, come pure il risarcimento dei danni, specie di tipo patrimoniale, che derivino dai fatti illeciti e siano comprovati dall'interessato in relazione ai disagi sopra illustrati;
- rende applicabile anche una sanzione penale qualora il trattamento illecito dei dati sia effettuato al fine di trarne per sé o per altri un profitto o per arrecare ad altri un danno, con la pena accessoria della pubblicazione della sentenza di condanna (artt. 35 e 38 legge n. 675).

4. MESSAGGI PUBBLICITARI A PROPRI CLIENTI

Per effetto del recepimento della direttiva 2002/58/CE sarà peraltro possibile integrare, nel prossimo futuro, la disciplina sopra illustrata, permettendo a talune società di far conoscere a propri clienti prodotti o servizi analoghi a quelli per i quali si è già stabilito un rapporto, con i medesimi clienti, di vendita di prodotti o servizi.
In tali casi, la società titolare del trattamento (dopo aver informato preventivamente e adeguatamente il cliente) potrà procedere all'invio del messaggio pubblicitario, offrendo però al cliente, in modo chiaro e distinto (sia al momento della raccolta dei suoi dati, sia in occasione di ciascun messaggio) il diritto di rifiutare sin dall'inizio tale uso dei dati o di obiettare, gratuitamente e in maniera agevole, anche successivamente (art. 13, par. 2, direttiva n. 2002/58/CE cit.)

5. MESSAGGI PER CONTO TERZI E ACQUISTO DI BANCHE DATI

In alcuni casi portati all'attenzione del Garante, l'invio di messaggi pubblicitari era stato effettuato, per conto di terzi committenti, da società specializzate che utilizzano indirizzi di posta elettronica contenuti in proprie banche dati.
Tali società, da considerarsi "titolari" o contitolari del trattamento dei dati a seconda del rapporto che si instaura con il committente e delle modalità di concreta utilizzazione dei dati, sono tenute a rispettare le disposizioni in tema di informativa e specifico consenso, anche per quanto riguarda l'eventuale comunicazione di dati personali ai committenti medesimi e le relative finalità.
Ciò comporta un quadro di obblighi e possibili responsabilità anche penali che gli operatori devono verificare con attenzione, anche uando la società specializzata incaricata sia stabilita fuori dell'Unione europea.
Dall'esame dei reclami e delle segnalazioni pervenuti al Garante è risultato, altresì, che alcuni dei soggetti che hanno utilizzato la posta elettronica per l'invio di messaggi pubblicitari avevano acquisito da terzi le banche dati contenenti gli indirizzi dei destinatari. In questi casi, chi acquisisce la banca dati deve accertare che ciascun interessato abbia validamente acconsentito alla comunicazione del proprio indirizzo di posta elettronica ed al suo successivo utilizzo ai fini di invio di materiale pubblicitario; al momento in cui registra i dati deve poi inviare in ogni caso, a tutti gli interessati, un messaggio di informativa che precisi gli elementi indicati nell'art. 10 della legge n. 675, comprensivi di un riferimento di luogo -e non solo di posta elettronica- presso cui l'interessato possa esercitare i diritti riconosciuti dalla legge.

6. DIRITTI DEGLI INTERESSATI

Indipendentemente dal rapporto esistente tra i mittenti ed i destinatari dei messaggi, chi detiene i dati deve assicurare in ogni caso agli interessati la possibilità di far valere in ogni momento i diritti riconosciuti dalla legge, i quali sono spesso esercitati per conoscere da quale fonte sono stati tratti i dati, o per far interrompere gratuitamente la loro ulteriore utilizzazione ai fini commerciali-pubblicitari, oppure per far cancellare i dati trattati in violazione di legge (art. 13, comma 1, lett. e), della legge).
Nel sito Internet del Garante è riportato un modello-tipo per esercitare tali diritti in maniera agevole, gratuitamente e senza particolari formalità, anche verbalmente o mediante posta elettronica, dimostrando la propria identità (art. 17, comma 1, d.P.R. n. 501 del 31 marzo 1998). Tale modello è utilizzabile in luogo di altri reperibili in reti telematiche che non sono pienamente validi in quanto si riferiscono anche ad aspetti non riconosciuti dall'art. 13 della legge n. 675 (ad esempio, chiedono il rilascio di attestazioni o la copia di autorizzazioni non previste).
I diritti vanno esercitati sulla base di tale modello direttamente presso l'indirizzo conoscibile del titolare o del responsabile del trattamento, riservando solo ad un'eventuale momento successivo l'instaurazione di una procedura contenziosa dinanzi al Garante o all'autorità giudiziaria.
Anche ai fini dell'esercizio di tali diritti, deve ritenersi che l'invio anonimo di messaggi pubblicitari senza l'indicazione di un mittente identificabile concreti già oggi un trattamento illecito di dati personali, a prescindere da quanto dispone il citato d.lg. n. 70/2003 sul commercio elettronico (come si è visto, fuori della materia della protezione dei dati personali) e da quanto, in riferimento ai dati personali, sarà previsto con il recepimento della direttiva n. 2002/58/CE (la quale non consente l'invio di messaggi pubblicitari quando l'identità del mittente viene camuffata o addirittura celata e quando non viene fornito un indirizzo valido che consenta al destinatario di richiedere la cessazione delle comunicazioni: art. 13, par. 4, dir. cit.).
I mittenti dei messaggi devono quindi indicare già oggi, in modo chiaro, la fonte di provenienza del messaggio, nonché il soggetto e l'indirizzo -non solo di posta elettronica- presso cui i destinatari possono esercitare i propri diritti (si veda, in proposito, l'art. 10, comma 1, lett. f) della legge n. 675). Appare altresì conforme al principio di correttezza indicare nell'oggetto del messaggio la sua tipologia pubblicitaria-commerciale (art. 9, comma 1, lett. a), legge n. 675).

7. ELENCHI DI POSSIBILI DESTINATARI

L'eventuale elenco predisposto da operatori, contenente i nominativi dei soggetti che non hanno manifestato il consenso o che lo hanno revocato (c.d. black list) non può essere utilizzato per porre a carico degli interessati, anche indirettamente, un onere di iscrizione nell'elenco medesimo.
Come si è illustrato, il consenso ha un connotato autorizzatorio "positivo" in base al quale l'eventuale silenzio dell'interessato omporta il diniego del consenso eventualmente richiesto e non rileva come assenso tacito all'invio dei messaggi.
Consta peraltro che alcuni operatori intendono adottare la diversa prassi di redigere anche tramite siti web appositi elenchi di persone che hanno manifestato il consenso, distinti in base alle diverse categorie di messaggi commerciali-pubblicitari che gli interessati hanno acconsentito a ricevere. Tale prassi, se correttamente seguita, può rappresentare una misura utile, sul piano organizzativo, per garantire un

più effettivo rispetto della volontà espressa dai singoli. A tale riguardo, costituirà una pratica utile quella di garantire agli interessati la possibilità di inserire direttamente il proprio nome nelle diverse liste o di cancellarlo dalle stesse, magari attraverso un'apposita pagina web, ferma restando l'esigenza di identificarli.

8. E-MAIL PROVENIENTI DALL'ESTERO
Ad alcuni messaggi, in quanto provenienti dall'estero, non è applicabile la legge italiana sulla protezione dei dati personali.
Ciò non comporta l'assoluta mancanza di rimedi o tutela, potendo l'utente chiedere una verifica da parte della competente autorità nazionale di protezione dei dati personali, ove istituita nel Paese eventualmente individuabile dal messaggio.
In altri casi, come quelli relativi alle leggi degli stati federali, l'invio di messaggi pubblicitari di posta elettronica può essere illecito in base alla legge di alcuni stati, per cui è parimenti possibile, per gli utenti, chiedere alle competenti autorità pubbliche degli stati di valutare la perseguibilità degli illeciti.
Va infine tenuto presente che alcune e-mail indesiderate possono essere lo strumento per commettere reati comuni (ad esempio di truffa) che devono considerarsi commessi nel territorio italiano quando, sebbene l'azione è avvenuta all'estero, l'evento-reato che ne deriva si è verificato in Italia.
Questa Autorità si riserva di valutare la posizione dei singoli fornitori di servizi i cui trattamenti sono stati oggetto di segnalazione, anche alla luce dell'ulteriore documentazione eventualmente pervenuta.
In questo quadro, con separati provvedimenti relativi all'esame dei singoli reclami e segnalazioni, si provvederà, oltre alle eventuali trasmissioni di atti all'autorità giudiziaria penale:
a) a contestare la violazione amministrativa relativa agli obblighi di informativa di cui all'art. 10 della legge 31 dicembre 1966, n. 675;
b) ad avviare il procedimento per l'applicazione delle ulteriori sanzioni amministrative previste dal d.lg. n. 185/1999;
TUTTO CIÒ PREMESSO IL GARANTE:
1. ai sensi dell'art. 31, comma 1, lett. l) della legge 31 dicembre 1996, n. 675, vieta l'ulteriore trattamento illecito di dati personali realizzato a scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva, effettuato in violazione delle disposizioni sopra richiamate da parte dei soggetti cui si riferiscono le segnalazioni e i reclami pervenuti;
2. ai sensi dell'art. 31, comma 1, lett. c) della legge 31 dicembre 1996, n. 675, segnala ai titolari del trattamento di cui agli atti del procedimento la necessità di conformare i trattamenti di dati personali ai principi richiamati nel presente provvedimento.
Roma, 29 maggio 2003
IL PRESIDENTE Rodotà
IL RELATORE Paissan
IL SEGRETARIO GENERALE Buttarelli

La responsabilità per il danneggiamento dei sistemi informativi.

NUMERO SCHEDA: 3419

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

FONTE: ITALIA OGGI

AUTORE: G. Di Rago; L. Giacopuzzi

DATA: 14/07/2003

PAGINA: 14-15

RIFERIMENTO NORMATIVO: l. 547/1993

NATURA ATTO: COMMENTO

Per le ipotesi di danni alle reti informatiche aziendali il nostro sistema prevede rilevanti responsabilità civili e penali non solo per i cosiddetti hackers, cioè i "pirati informatici", autori di attacchi dall'esterno delle aziende, ma anche nei confronti dei titolari delle stesse che non hanno adottato le misure di sicurezza necessarie per proteggere i propri sistemi e per i dipendenti.
Punto di riferimento è la legge 547/1993 che ha apportato delle modifiche al codice penale e al codice di procedura penale per aggiungere fattispecie specifiche relative alla criminalità informatica.
L'art. 491 bis contiene la definizione di documento informatico.
Fra le ipotesi specifiche di reato se ne citano, a titolo di esempio, alcune:
- "accesso abusivo a un sistema informatico o telematico" (art. 615 ter c.p.);
"intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche" (art. 617 quater c.p.);
"frode informatica" (art. 640 ter c.p.).
La modifica all'art. 268 del codice di procedura penale è finalizzata soprattutto a facilitare la raccolta delle prove.
La legislazione sulla privacy prevede sanzioni penali per coloro che trattano dati personali senza avere adottato tutte le misure minime di sicurezza (l. 675/1996; d.p.r. 318/1999).
Per quanto concerne la responsabilità civile si applicano le disposizioni degli articoli 2043 e seguenti.
Per quanto riguarda la responsabilità del provider (cioè la persona fisica o giuridica che presta un servizio della società dell'informazione), punto di riferimento è il d.lgs. 70/2003 (Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare rifeimento al commercio elettronico).

E' stato costituito il Comitato Tecnico Nazionale sulla Sicurezza Informatica nella Pubblica Amministrazione

NUMERO SCHEDA: 1972

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI E SICUREZZA INFORM.

RIFERIMENTO NORMATIVO: direttiva 16/01/2002

NATURA ATTO: DECRETO

DATA ATTO: 24/07/2002

ORGANO: MINISTERI

Il Comitato Tecnico Nazionale sulla Sicurezza Informatica nella P.A, istituito con decreto interministeriale del 24 luglio 2002, è stato costituito presso il Dipartimento per l'Innovazione e le Tecnologie. Il Comitato avra' fra i compiti la riduzione delle vulnerabilita' dei sistemi

informatici, la garanzia di integrita' ed affidabilita' dell'informazione pubblica e quello di creare e mantenere una posizione primaria a livello europeo.
Il Comitato è stato presentato il 16 ottobre 2002 dal Ministro per l'Innovazione e le Tecnologie e dal Ministro delle Comunicazioni e rappresenta uno dei primi esempi di attuazione della raccomandazione dell'Unione Europea, indirizzata alle Pubbliche Amministrazioni dei singoli Paesi membri, per avviare misure di sicurezza efficaci per il conseguimento di una base minima di sicurezza informatica nell'erogazione dei servizi, soprattutto quando si tratta di sistemi che saranno sempre più caratterizzati da interoperatività e cooperazione.
La creazione del Comitato rappresenta, una fase degli interventi suggeriti dalla direttiva d16 gennaio 2002 del Ministro per l'Innovazione e le Tecnologie di concerto con il dicastero delle Comunicazioni sulla sicurezza ICT per le Pubbliche Amministrazioni. La direttiva, che recepisce le indicazioni dell'Unione europea, raccomanda "di avviare nell'immediato alcune azioni prioritarie tali da consentire il conseguimento di un primo importante risultato di allineamento ad una base minima di sicurezza".
Il Dipartimento per l'Innovazione e le Tecnologie ha pubblicato sul proprio sito Internet il decreto interministeriale che istituisce il Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni. :
http://www.innovazione.gov.it/ita/intervento/normativa/allegati/dm_240702.pdf

Il Parlamento europeo ha approvato la nuova direttiva relativa al trattamento dei dati personali e alla tutela della vita privata, nel settore delle comunicazioni elettroniche.

NUMERO SCHEDA: 1726

CLASSIFICAZIONE: INFORMAZIONE E COMUNICAZIONE

SOTTOCLASSIFICAZIONE: Telecomunicazioni

FONTE: ITALIA OGGI

DATA: 10/08/2002

RIFERIMENTO NORMATIVO: direttiva 97/66/CE; d.lgs. 171/98

NATURA ATTO: DIRETTIVA C.E.

DATA ATTO: 12/07/2002

NUM. ATTO: 58

ORGANO: PARLAMENTO

Il Parlamento europeo ha approvato la direttiva 2002/58/CE sul trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche, che è entrata in vigore il 31 luglio 2002. Gli Stati membri dovranno conformarsi alle nuove disposizioni europee entro il 31 ottobre 2003.

La nuova direttiva sostituisce la 97/66/CE (attuata in Italia con il d.lgs. 171/98) mantenendo elevato il livello di protezione dei dati personali e della vita privata da questa garantito.
Il nuovo testo riprende gran parte delle disposizioni della direttiva vigente apportando variazioni indispensabili a seguito degli sviluppi intervenuti nei servizi e nelle tecnologie delle comunicazioni elettroniche. L'adeguamento permetterà ad utenti e consumatori di godere effettivamente di uno stesso livello di tutela, qualunque sia la tecnologia utilizzata per la fornitura del servizio (definito non più di telecomunicazioni ma più correttamente di comunicazioni elettroniche).
Il Parlamento europeo sottolinea che la necessità di adeguare la vecchia direttiva 97/66/CE nasce dagli sviluppi che si sono verificati nei mercati e nelle tecnologie dei servizi di comunicazione elettronica tenendo conto che l'accesso ad Internet apre nuove possibilità agli utenti, ma rappresenta anche nuovi pericoli per i loro dati personali e per la loro vita privata. Analogamente l'uso di software spia (spyware), o di bachi invisibili (web bug), che possono introdursi nel terminale e permettere di accedere illecitamente e in modo non trasparente ad informazioni, o di seguire gli spostamenti in rete dell'utente, può rappresentare una grave intrusione nella vita privata e deve essere consentito unicamente per scopi legittimi e informando previamente l'interessato.
Le principali novità introdotte dalla nuova direttiva europea riguardano:
- l'invio di e-mail commerciali e pubblicitarie solo agli utenti che abbiano espresso il proprio consenso: infatti l'iscrizione negli elenchi telefonici pubblici, cartacei o elettronici, può avvenire solo con il consenso degli abbonati e secondo modalità da loro scelte;
- il divieto di inviare messaggi di posta elettronica, a scopo commerciale o pubblicitario, omettendo o camuffando l'identità del mittente o senza l'indicazione di un indirizzo valido, cui il destinatario possa inviare una richiesta di cessazione.
- la regolamentazione dell'uso di cookies, spyware e bug.
- una particolare tutela per i dati relativi alla localizzazione dei cellulari raccolti nel corso della fornitura di nuovi tipi di servizi erogati da reti cellulari e satellitari che consentono di individuare esattamente l'apparecchiatura terminale dell'utente.

Nella direttiva si sollecita, inoltre, la progettazione di sistemi di fornitura di reti e servizi di comunicazione che limitino al minimo la quantità di dati personali necessari. Si prevede che i dati dei naviganti in Internet possano essere conservati dopo l'erogazione del servizio per il quale sono stati forniti, al pari di quelli delle chiamate telefoniche, ai fini della fatturazione e del pagamento per interconnessione.
Per quanto riguarda il settore della telefonia la direttiva conferma il principio generale, già affermato nella 97/66/CE, che i dati sul traffico dell'utente devono essere cancellati o resi anonimi al termine della comunicazione. Permette comunque, entro precisi limiti e sulla base di determinate garanzie, la possibilità di introdurre delimitati tempi di conservazione dove vi siano necessità di interventi proporzionali per finalità di accertamento e prevenzione di reati o motivi di sicurezza nazionale.

Si allega il testo integrale della direttiva:

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio
del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

Articolo 1
Finalità e campo d'applicazione

1. La presente direttiva armonizza le disposizioni degli Stati membri necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità.
2. Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva 95/46/CE. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche.
3. La presente direttiva non si applica alle attività che esulano dal campo di applicazione del trattato che istituisce la Comunità europea, quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale.

Articolo 2
Definizioni

Salvo diversa disposizione, ai fini della presente direttiva si applicano le definizioni di cui alla direttiva 95/46/CE e alla direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica (direttiva quadro)(8).
Si applicano inoltre le seguenti definizioni:
a) "utente": qualsiasi persona fisica che utilizzi un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
b) "dati relativi al traffico": qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
c) "dati relativi all'ubicazione": ogni dato trattato in una rete di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
d) "comunicazione": ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse, come parte di un servizio di radiodiffusione, al pubblico tramite una rete di comunicazione elettronica salvo quando le informazioni possono essere collegate all'abbonato o utente che riceve le informazioni che può essere identificato;
e) "chiamata": la connessione istituita da un servizio telefonico accessibile al pubblico che consente la comunicazione bidirezionale in tempo reale;
f) "consenso" dell'utente o dell'abbonato: corrisponde al consenso della persona interessata di cui alla direttiva 95/46/CE;
g) "servizio a valore aggiunto": il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
h) "posta elettronica": messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente fino a che il ricevente non ne ha preso conoscenza.

Articolo 3
Servizi interessati

1. La presente direttiva si applica al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nella Comunità.
2. Gli articoli 8, 10 e 11 si applicano alle linee di abbonati collegate a centrali telefoniche digitali e, qualora sia tecnicamente possibile e non richieda un onere economico sproporzionato, alle linee di abbonati collegate a centrali telefoniche analogiche.
3. Gli Stati membri notificano alla Commissione i casi in cui l'osservanza delle prescrizioni di cui agli articoli 8, 10 e 11 risulti tecnicamente impossibile o richieda un onere economico sproporzionato.

Articolo 4
Sicurezza

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico deve prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete. Tenuto conto delle attuali conoscenze in materia e dei loro costi di realizzazione, dette misure assicurano un livello di sicurezza adeguato al rischio esistente.
2. Nel caso in cui esista un particolare rischio di violazione della sicurezza della rete, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha l'obbligo di informarne gli abbonati indicando, qualora il rischio sia al di fuori del campo di applicazione delle misure che devono essere prese dal fornitore di servizio, tutti i possibili rimedi, compresi i relativi costi presumibili.

Articolo 5
Riservatezza delle comunicazioni

1. Gli Stati membri assicurano, mediante disposizioni di legge nazionali, la riservatezza delle comunicazioni effettuate tramite la rete pubblica di comunicazione e i servizi di comunicazione elettronica accessibili al pubblico, nonché dei relativi dati sul traffico. In particolare essi vietano l'ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza.
2. Il paragrafo 1 non pregiudica la registrazione legalmente autorizzata di comunicazioni e dei relativi dati sul traffico se effettuata nel quadro di legittime prassi commerciali allo scopo di fornire la prova di una transazione o di una qualsiasi altra comunicazione commerciale.
3. Gli Stati membri assicurano che l'uso di reti di comunicazione elettronica per archiviare informazioni o per avere accesso a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente interessato sia stato informato in modo chiaro e completo, tra l'altro, sugli scopi del trattamento in conformità della direttiva 95/46/CE e che gli sia offerta la possibilità di rifiutare tale trattamento da parte del responsabile del trattamento. Ciò non impedisce l'eventuale memorizzazione tecnica o l'accesso al solo fine di effettuare o facilitare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria a fornire un servizio della società dell'informazione esplicitamente richiesto dall'abbonato o dall'utente.

Articolo 6
Dati sul traffico

1. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1.
2. I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento.
3. Ai fini della commercializzazione dei servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, il fornitore di un servizio di comunicazione elettronica accessibile al pubblico ha facoltà di sottoporre a trattamento i dati di cui al paragrafo 1 nella misura e per la durata necessaria per siffatti servizi, o per la commercializzazione, sempre che l'abbonato o l'utente a cui i dati si riferiscono abbia dato il proprio consenso. Gli abbonati o utenti hanno la possibilità di ritirare il loro consenso al trattamento dei dati relativi al traffico in qualsiasi momento.
4. Il fornitore dei servizi deve informare l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del trattamento ai fini enunciati al paragrafo 2 e, prima di ottenere il consenso, ai fini enunciati al paragrafo 3.

5. Il trattamento dei dati relativi al traffico ai sensi dei paragrafi da 1 a 4 deve essere limitato alle persone che agiscono sotto l'autorità dei fornitori della rete pubblica di comunicazione elettronica e dei servizi di comunicazione elettronica accessibili al pubblico che si occupano della fatturazione o della gestione del traffico, delle indagini per conto dei clienti, dell'accertamento delle frodi, della commercializzazione dei servizi di comunicazione elettronica o della prestazione di servizi a valore aggiunto. Il trattamento deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività.
6. I paragrafi 1, 2, 3 e 5 non pregiudicano la facoltà degli organismi competenti di ottenere i dati relativi al traffico in base alla normativa applicabile al fine della risoluzione delle controversie, in particolare di quelle attinenti all'interconnessione e alla fatturazione.

Articolo 7
Fatturazione dettagliata

1. Gli abbonati hanno diritto di ricevere fatture non dettagliate.
2. Gli Stati membri applicano norme nazionali per conciliare i diritti degli abbonati che ricevono fatture dettagliate con il diritto alla vita privata degli utenti chiamanti e degli abbonati chiamati, ad esempio garantendo che detti utenti e abbonati possano disporre, per le comunicazioni e per i pagamenti, di sufficienti modalità alternative che tutelino maggiormente la vita privata.

Articolo 8
Presentazione e restrizione dell'identificazione della linea chiamante e collegata

1. Qualora sia disponibile la presentazione dell'identificazione della linea chiamante, il fornitore dei servizi deve offrire all'utente chiamante la possibilità di impedire, mediante una funzione semplice e gratuitamente, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata. L'abbonato chiamante deve avere tale possibilità linea per linea.
2. Qualora sia disponibile la presentazione dell'identificazione della linea chiamante, il fornitore di servizi deve offrire all'abbonato chiamato la possibilità, mediante una funzione semplice e gratuitamente, per ogni ragionevole utilizzo di tale funzione, di impedire la presentazione dell'identificazione delle chiamate entranti.
3. Qualora sia disponibile la presentazione dell'identificazione della linea chiamante e tale indicazione avvenga prima che la comunicazione sia stabilita, il fornitore di servizi deve offrire all'abbonato chiamato la possibilità, mediante una funzione semplice, di respingere le chiamate entranti se la presentazione dell'identificazione della linea chiamante è stata eliminata dall'utente o abbonato chiamante.
4. Qualora sia disponibile la presentazione dell'identificazione della linea collegata, il fornitore di servizi deve offrire all'abbonato chiamato la possibilità di impedire, mediante una funzione semplice e gratuitamente, la presentazione dell'identificazione della linea collegata all'utente chiamante.
5. Il paragrafo 1 si applica anche alle chiamate provenienti dalla Comunità e dirette verso paesi terzi. I paragrafi 2, 3 e 4 si applicano anche alle chiamate in entrata provenienti da paesi terzi.
6. Gli Stati membri assicurano che, qualora sia disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, il fornitore di servizi di comunicazione elettronica accessibili al pubblico informi quest'ultimo di tale possibilità e delle possibilità di cui ai paragrafi 1, 2, 3 e 4.

Articolo 9
Dati relativi all'ubicazione diversi dai dati relativi al traffico

1. Se i dati relativi all'ubicazione diversi dai dati relativi al traffico, relativi agli utenti o abbonati di reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico possono essere sottoposti a trattamento, essi possono esserlo soltanto a condizione che siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto. Prima di chiedere il loro consenso, il fornitore del servizio deve informare gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti a trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto. Gli utenti e gli abbonati devono avere la possibilità di

ritirare il loro consenso al trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico in qualsiasi momento.
2. Se hanno dato il consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, l'utente e l'abbonato devono continuare ad avere la possibilità di negare, in via temporanea, mediante una funzione semplice e gratuitamente, il trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni.
3. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico ai sensi di paragrafi 1 e 2 deve essere limitato alle persone che agiscono sotto l'autorità del fornitore della rete pubblica di telecomunicazione o del servizio di comunicazione elettronica accessibile al pubblico o del terzo che fornisce il servizio a valore aggiunto, e deve essere circoscritto a quanto è strettamente necessario per la fornitura di quest'ultimo.

Articolo 10
Deroghe

Gli Stati membri assicurano che esistano procedure trasparenti in base alle quali il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico:
a) possa annullare, in via temporanea, la soppressione della presentazione dell'identificazione della linea chiamante a richiesta di un abbonato che chieda la presentazione dell'identificazione di chiamate malintenzionate o importune. In tal caso, in base al diritto nazionale, i dati che identificano l'abbonato chiamante sono memorizzati e resi disponibili dal fornitore di una rete pubblica di comunicazioni e/o di un servizio di comunicazioni elettroniche accessibile al pubblico;
b) possa annullare la soppressione della presentazione dell'identificazione della linea chiamante e possa sottoporre a trattamento i dati relativi all'ubicazione, nonostante il rifiuto o il mancato consenso temporanei dell'abbonato o dell'utente, linea per linea, per gli organismi che trattano chiamate di emergenza, riconosciuti come tali da uno Stato membro, in particolare per le forze di polizia, i servizi di ambulanza e i vigili del fuoco, affinché questi possano reagire a tali chiamate.

Articolo 11
Trasferimento automatico della chiamata

Gli Stati membri provvedono affinché ciascun abbonato abbia la possibilità, gratuitamente e mediante una funzione semplice, di bloccare il trasferimento automatico delle chiamate verso il proprio terminale da parte di terzi.

Articolo 12
Elenchi di abbonati

1. Gli Stati membri assicurano che gli abbonati siano informati, gratuitamente e prima di essere inseriti nell'elenco, in merito agli scopi degli elenchi cartacei o elettronici a disposizione del pubblico o ottenibili attraverso i servizi che forniscono informazioni sugli elenchi, nei quali possono essere inclusi i loro dati personali, nonché in merito ad ogni ulteriore possibilità di utilizzo basata su funzioni di ricerca incorporate nelle versioni elettroniche degli elenchi stessi.
2. Gli Stati membri assicurano che gli abbonati abbiano la possibilità di decidere se i loro dati personali - e, nell'affermativa, quali - debbano essere riportati in un elenco pubblico, sempreché tali dati siano pertinenti per gli scopi dell'elenco dichiarati dal suo fornitore. Gli Stati membri provvedono affinché gli abbonati abbiano le possibilità di verificare, rettificare o ritirare tali dati. Il fatto che i dati non siano riportati in un elenco pubblico di abbonati la verifica, la correzione o il ritiro dei dati non devono comportare oneri.
3. Gli Stati membri possono disporre che sia chiesto il consenso ulteriore degli abbonati per tutti gli scopi di un elenco pubblico diversi dalla ricerca di dati su persone sulla base del loro nome e, ove necessario, di un numero minimo di altri elementi di identificazione.
4. I paragrafi 1 e 2 si applicano agli abbonati che siano persone fisiche. Gli Stati membri assicurano inoltre, nel quadro del diritto comunitario e della normativa nazionale applicabile, un'adeguata tutela degli interessi legittimi degli abbonati che non siano persone fisiche relativamente all'inclusione negli elenchi pubblici.

Articolo 13

Comunicazioni indesiderate

1. L'uso di sistemi automatizzati di chiamata senza intervento di un operatore (dispositivi automatici di chiamata), del telefax o della posta elettronica a fini di commercializzazione diretta è consentito soltanto nei confronti degli abbonati che abbiano espresso preliminarmente il loro consenso.
2. Fatto salvo il paragrafo 1, allorché una persona fisica o giuridica ottiene dai suoi clienti le coordinate elettroniche per la posta elettronica nel contesto della vendita di un prodotto o servizio ai sensi della direttiva 95/46/CE, la medesima persona fisica o giuridica può utilizzare tali coordinate elettroniche a scopi di commercializzazione diretta di propri analoghi prodotti o servizi, a condizione che ai clienti sia offerta in modo chiaro e distinto al momento della raccolta delle coordinate elettroniche e ad ogni messaggio la possibilità di opporsi, gratuitamente e in maniera agevole, all'uso di tali coordinate elettroniche qualora il cliente non abbia rifiutato inizialmente tale uso.
3. Gli Stati membri adottano le misure appropriate per garantire che, gratuitamente, le comunicazioni indesiderate a scopo di commercializzazione diretta, in casi diversi da quelli di cui ai paragrafi 1 e 2, non siano permesse se manca il consenso degli abbonati interessati oppure se gli abbonati esprimono il desiderio di non ricevere questo tipo di chiamate; la scelta tra queste due possibilità è effettuata dalla normativa nazionale.
4. In ogni caso, è vietata la prassi di inviare messaggi di posta elettronica a scopi di commercializzazione diretta camuffando o celando l'identità del mittente da parte del quale la comunicazione è effettuata, o senza fornire un indirizzo valido cui il destinatario possa inviare una richiesta di cessazione di tali comunicazioni.
5. Le disposizioni di cui ai paragrafi 1 e 3 si applicano agli abbonati che siano persone fisiche. Gli Stati membri garantiscono inoltre, nel quadro del diritto comunitario e della normativa nazionale applicabile, un'adeguata tutela degli interessi legittimi degli abbonati che non siano persone fisiche relativamente alle comunicazioni indesiderate.

Articolo 14
Caratteristiche tecniche e normalizzazione

1. Salvo quanto disposto nei paragrafi 2 e 3, nell'attuare le disposizioni della presente direttiva gli Stati membri assicurano che non siano imposti, per i terminali o altre apparecchiature di comunicazione elettronica, norme inderogabili relative a caratteristiche tecniche specifiche che possano ostacolare l'immissione sul mercato e la libera circolazione di tali apparecchiature tra i vari Stati membri e al loro interno.
2. Qualora talune disposizioni della presente direttiva possano essere attuate soltanto attraverso la prescrizione di caratteristiche tecniche specifiche per le reti di comunicazione elettronica, gli Stati membri informano la Commissione secondo le procedure di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, che prevede una procedura di informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione(9).
3. All'occorrenza, possono essere adottate misure dirette a garantire che le apparecchiature terminali siano costruite in maniera compatibile con il diritto degli utenti di tutelare e controllare l'uso dei loro dati personali in conformità della direttiva 1999/5/CE e della decisione 87/95/CEE del Consiglio, del 22 dicembre 1986, relativa alla normalizzazione nel settore delle tecnologie dell'informazione delle telecomunicazioni(10).

Articolo 15
Applicazione di alcune disposizioni della direttiva 95/46/CE

1. Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi

generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.
2. Le disposizioni del capo III della direttiva 95/46/CE relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa.
3. Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, svolge i compiti di cui all'articolo 30 della direttiva stessa anche per quanto concerne materie disciplinate dalla presente direttiva, segnatamente la tutela dei diritti e delle libertà fondamentali e degli interessi legittimi nel settore delle comunicazioni elettroniche.

Articolo 16
Disposizioni transitorie
1. L'articolo 12 non si applica agli elenchi già prodotti o immessi sul mercato su supporto cartaceo o elettronico off-line prima dell'entrata in vigore delle disposizioni nazionali adottate in forza della presente direttiva.
2. Se i dati personali degli abbonati a servizi pubblici fissi o mobili di telefonia vocale sono stati inseriti in un elenco pubblico degli abbonati in conformità con le disposizioni della direttiva 95/46/CE e dell'articolo 11 della direttiva 97/66/CE prima dell'entrata in vigore delle disposizioni nazionali adottate conformemente alla presente direttiva, i dati personali di tali abbonati possono restare inseriti in tale elenco pubblico cartaceo o elettronico, comprese le versioni con funzioni di ricerca inverse, salvo altrimenti da essi comunicato dopo essere stati pienamente informati degli scopi e delle possibilità in conformità con l'articolo 12 della presente direttiva.

Articolo 17
Attuazione della direttiva

1. Gli Stati membri mettono in vigore le disposizioni necessarie per conformarsi alla presente direttiva entro il 31 ottobre 2003. Essi ne informano immediatamente la Commissione.
Quando gli Stati membri adottano tali disposizioni, queste contengono un riferimento alla presente direttiva o sono corredate da un siffatto riferimento all'atto della loro pubblicazione ufficiale. Le modalità di tale riferimento sono decise dagli Stati membri.
2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni di diritto interno che essi adottano nel settore disciplinato dalla presente direttiva, nonché ogni loro successiva modificazione ed integrazione.

Articolo 18
Riesame

La Commissione presenta al Parlamento europeo e al Consiglio, non oltre tre anni dalla data di cui all'articolo 17, paragrafo 1, una relazione sull'applicazione della presente direttiva e il relativo impatto sugli operatori economici e suoi consumatori, in particolare per quanto riguarda le disposizioni sulle comunicazioni indesiderate, tenendo conto dell'ambiente internazionale. A tale fine, la Commissione può chiedere agli Stati membri informazioni che saranno fornite senza ritardi ingiustificati. Ove opportuno, la Commissione presenta proposte di modifica della presente direttiva, tenendo conto dei risultati di detta relazione, di ogni modifica del settore e di ogni altra proposta che ritenga necessaria per migliorare l'efficacia della presente direttiva.

Articolo 19
Abrogazione

La direttiva 97/66/CE è abrogata con efficacia a decorrere dalla data di applicazione di cui all'articolo 17, paragrafo 1.
I riferimenti alla direttiva abrogata si intendono fatti alla presente direttiva.

Articolo 20
Entrata in vigore

La presente direttiva entra in vigore il giorno della pubblicazione nella Gazzetta ufficiale delle Comunità europee.

Articolo 21
Destinatari

Gli Stati membri sono destinatari della presente direttiva.
Fatto a Bruxelles, addì 12 luglio 2002.
Per il Parlamento europeo
Il Presidente
P. Cox
Per il Consiglio
Il Presidente
T. Pedersen

L'introduzione contro la volontà del titolare fa scattare la responsabilità dell'hacker.

NUMERO SCHEDA: 396

CLASSIFICAZIONE: INFORMATICA

SOTTOCLASSIFICAZIONE: REATI INFORMATICI

FONTE: GUIDA AL DIRITTO

AUTORE: Paolo Galdieri

NUMERO: 8

DATA: 03/06/2001

PAGINA: 81-82

RIFERIMENTO NORMATIVO: legge 23 dicembre 1993 n.547

NATURA ATTO: COMMENTO

Con la decisione n.12732/2000 la Suprema Corte sottolinea come "la violazione dei dispositivi di protezione del sistema informatico non assuma rilevanza di per sé, bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone". Sempre a parere della Corte, si tratterebbe "di un illecito caratterizzato, appunto dalla contravvenzione alle disposizioni del titolare, come avviene nel delitto di violazione di domicilio", da cui questa disposizione sicuramente discende. Oggetto di valutazione della decisione suddetta è l'articolo 615-ter del codice penale (accesso abusivo a un sistema informatico o telematico), inserito all'interno del codice penale dalla legge 23 dicembre 1993 n.547 ("Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica").

- E' a disposizione il testo del commento presso il Settore Studi e Documentazione legislativi.

Si allega il testo della sentenza.

Corte di Cassazione - Sezione V Penale
Sentenza n. 12732 del 6 dicembre 2000

REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO
LA CORTE SUPREMA DI CASSAZIONE
SEZIONE V PENALE

Composta dai signori magistrati:
Presidente B.Foscarini
Relatore A.Nappi

MOTIVI DELLA DECISIONE

Con la sentenza impugnata la Corte d'appello di Torino confermò la dichiarazione di colpevolezza di A.Z. e di D. M. in ordine al delitto di accesso abusivo al sistema informatico della (omissis)., gestrice di contabilità per conto terzi, e dichiarò colpevole del massimo reato, quale autore materiale dei fatti, il programmatore V. B., che in primo grado ne era stato assolto per difetto di dolo.
Risulta dalle sentenze di merito che A. Z., già socio di F. V. nella (omissis), nel 1994 era uscito dalla società per intraprendere analoga attività con il commercialista D. M., già collaboratore esterno della (omissis), e, non avendo ottenuto di poter utilizzare come locatario l'impianto informatico della società, ne aveva copiato i dati su un analogo calcolatore con l'aiuto di V. B., facilitandosi così l'acquisizione di un gran numero di clienti della (omissis).
Ricorrono per cassazione gli imputati, che hanno proposto cinque motivi di impugnazione. Con il primo motivo i ricorrenti lamentano mancanza di motivazione sul motivo d'appello con il quale era stato dedotto che V. B. e il suo datore di lavoro V. C., proprietario del programma concesso in uso sia alla (omissis) sia a A. Z. e D. M., avevano diritto di copiare e modificare il software. E con il connesso terzo motivo si lamenta che i giudici d'appello abbiano omesso di considerare il fatto, ben valorizzato invece dal tribunale, che V. B. agiva su disposizioni di V. C. e non aveva motivo di dubitare della legittimità di tali disposizioni anche con riferimento alle copie effettuate in favore di A. Z. e D.M..
Con il secondo motivo i ricorrenti deducono violazione dell'art.615 ter c.p.[1], lamentando che i giudici del merito abbiano ritenuto configurabile il reato contestato anche in mancanza di protezioni di sicurezza interne al sistema, mentre la dottrina è concorde nell'escludere la rilevanza di protezioni esterne.
Con il quarto motivo i ricorrenti deducono mancanza di motivazione in ordine alla determinazione della pena, irrogata in misura identica a tutti gli imputati, senza alcuna considerazione per e diverse posizioni soggettive.
Con il quinto motivo infine i ricorrenti deducono violazione dell'art.538 comma 1 c.p.p., lamentando che i giudici del merito si siano pronunciati su una domanda in realtà non proposta dalla parte civile (omissis), che, costituitasi per il reato di cui all'art. 640 ter c.p.originariamente contestato, non aveva rinnovato la costituzione anche per il reato di cui all'art.615 ter c.p., contestato in udienza.
I motivi del ricorso sono stati successivamente illustrati con ampia memoria depositata il 10 maggio 2000.
Una memoria è stata altresì depositata dalla parte civile.

Il ricorso deve essere rigettato.
Il primo motivo del ricorso, come il motivo d'appello cui si riferisce per lamentarne l'immotivato Rigetto, non distingue tra il programma informatico, di cui si assume fosse proprietario V. C., e i dati informatici, non del software.Sicchè era manifestamente infondato il motivo d'appello con il quale si deduceva l'inesistenza del reato in relazione al diritto di C., del proprietario del programma, di copiarlo e aggiornarlo. E secondo una consolidata giurisprudenza di questa Corte, deve essere considerato privo di fondamento il motivo del ricorso per cassazione con il quale si deduce mancanza di motivazione in ordine ad un motivo d'appello inammissibile o manifestamente infondato (Cass., sez 1, 23 marzo 1987, Imbimbo, m. 176707, Cass., sez1, 28 settembre 1987, Cisco, m. 177007, Cass., sez 4 , 26 settembre 1990, Pilloni, m. 185682, Cass., sez 1, 5 marzo 1991, Calò, m. 186972, Cass., sez 5, 18 febbraio 1992, Cremonini, m. 189818, Cass., sez 1, 28 marzo1996, Bruno, m. 204548).

Ne consegue anche l'inammissibilità, per violazione dell'art.606 comma 3 c.p.p., del terzo motivo del ricorso, con il quale si lamenta l'erronea affermazione della responsabilità di V. B., perché, una volta chiarita la distinzione tra i dati informatici e il programma destinato a elaborarli, la censura rimane riferibile a una mera valutazione di merito circa la consapevolezza da parte dell'imputato di una tale distinzione e della conseguente illiceità della copia dei dati.
Il secondo motivo del ricorso pone il problema della natura della protezione di sicurezza rilevante ai fini della configurabilità del delitto previsto dall'art.615 ter c.p..
La corte d'appello ha ritenuto che, ai fini della configurabilità del reato, assumano rilevanza non solo le protezioni interne al sistema informatico, come le chiavi d'accesso, ma anche le protezioni esterne, come la custodia degli impianti, in particolare quando, come nel caso in esame, si tratti di banche dati private, per definizione interdette a coloro che sono estranei all'impresa che le gestisce.
I ricorrenti sostengono, invece, che soltanto la protezione interna al sistema è idonea a manifestare la volontà del proprietario di escludere terzi, come dimostrerebbe il fatto che il D.P.R. n. 318 del 1999 richiede come necessaria una chiave d'accesso nel trattamento dei dati personali.
Il motivo di ricorso è infondato.
L'art. 615 ter comma 1 c.p. punisce non solo chi s'introduce abusivamente in un sistema informatico o telematico, ma anche chi vi si mantiene contro la volontà esplicita o tacita di chi ha il diritto di escluderlo.
Ne consegue che la violazione dei dispositivi di protezione del sistema informatico non assume rilevanza di per se, bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone.
Non si tratta perciò di un illecito caratterizzato dall'effrazione dei sistemi protettivi, perchè altrimenti non avrebbe rilevanza la condotta di chi, dopo essere legittimamente entrato nel sistema informatico, vi si mantenga contro la volontà del titolare. Ma si tratta di un illecito caratterizzato appunto dalla contravvenzione alle disposizioni del titolare, come avviene nel delitto di violazione di domicilio, che è stato notoriamente il modello di questa nuova fattispecie penale, tanto da indurre molti a individuarvi, talora anche criticamente, la tutela di un domicilio informatico.
Certo è necessario che l'accesso al sistema informatico non sia aperto a tutti, come talora avviene soprattutto quando si tratti di sistemi telematici. Ma deve ritenersi che, ai fini della configurabilità del delitto, assuma rilevanza qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso al sistema informatico, anche quando si tratti di strumenti esterni al sistema e meramente organizzativi, in quanto destinati a regolare l'ingresso stesso nei locali in cui gli impianti sono custoditi. Ed è certamente corretta, in questa prospettiva, la distinzione operata dalla corte d'appello tra le banche dati offerte al pubblico a determinate condizioni e le banche dati destinate a un'utilizzazione privata esclusiva, come i dati contabili di un'azienda.
In questo secondo caso è evidente, infatti, che, anche in mancanza di meccanismi di protezione informatica, commette il reato la persona estranea all'organizzazione che acceda ai dati senza titolo o autorizzazione, essendo implicita, ma intuibile, la volontà dell'avente diritto di escludere gli estranei.
D'altro canto, l'analogia con la fattispecie della violazione di domicilio deve indurre a concludere integri la fattispecie criminosa anche chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Infatti, se l'accesso richiede un'autorizzazione e questa e questa è destinata a un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva. Sicchè correttamente i giudici del merito hanno ritenuto configurabile il reato nella condotta di V. B.,che, autorizzato all'accesso per controllare la funzionalità del programma informatico, si avvalse dell'autorizzazione per copiare i dati dal quel programma gestiti .
Privo di qualsiasi pertinenza al caso in esame è, infine, il regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'art. 15 comma 2 della legge 31 dicembre 1996, n. 675. Infatti la mancata adozione delle misure minime di sicurezza nel trattamento dei dati personali è prevista come reato dall'art.36 della legge n. 675 del 1996; ma evidentemente la consumazione di questo reato non esime, comunque, da responsabilità chi violi i pur insufficienti meccanismi di protezione esistenti.
Il quarto motivo del ricorso è inammissibile per violazione dell'art. 606 comma 3 c.p.p., perché propone censure attinenti al merito della decisione impugnata, congruamente giustificata con riferimento alla ritenuta gravità della violazione del rapporto fiduciario con la parte lesa, comune a tutti gli imputati.
Come s'è detto, con il quinto motivo i ricorrenti deducono violazione dell'art.538 c.p.p., lamentando che i giudici del merito si siano pronunciati su una domanda di risarcimento danni non proposta dalla parte civile per il reato di cui all'art. 615 ter c.p., contestato in udienza.

Tuttavia gli stessi ricorrenti riconoscono che, sin dal primo grado del giudizio, la parte civile concluse chiedendo la condanna degli imputati al risarcimento anche dei danni derivanti dal reato previsto dall'art.615 ter c.p.; sicchè non si può dire che i giudici del merito si siano pronunciati su una domanda non proposta.

In realtà i ricorrenti pongono una questione diversa da quella formalmente enunciata, perché essi lamentano che per il nuovo reato contestato in udienza non v'era stata costituzione di parte civile; e sostengono che una tale rinnovata costituzione sarebbe stata invece necessaria, secondo quanto previsto anche dalla sentenza n. 98 del 1996 della Corte Costituzionale.
Sennonchè la giurisprudenza di questa Corte, richiamata anche dalla Corte Costituzionale, ha ben chiarito che occorre distinguere tra la posizione della persona offesa non costituita, che in caso di nuove contestazioni ha diritto alla sospensione del dibattimento onde poter eventualmente costituire parte civile per la nuova udienza, e il caso della persona offesa già ma solo in vista della possibile modifica, sotto il profilo tanto della causa petendi quanto del petitum, del già costituito rapporto processuale (Cass., sez III, 27 settembre 1995, Roncati). Sicchè, per la parte civile già costituita non occorre rinnovare la costituzione in relazione al nuovo reato contestato in udienza all'imputato, ma è sufficiente modificare la domanda già proposta. E nel caso in esame deve ritenersi che un idoneo aggiornamento della domanda si ebbe appunto con la formulazione delle conclusioni in chiusura del dibattito di primo grado.
Il ricorso va pertanto, rigettato.

P.Q.M.

La Corte rigetta il ricorso e condanna i ricorrenti in solido al pagamento delle spese del procedimento e inoltre al rimborso delle spese in favore della parte civile, liquidate in complessive £ 2.306.000, di cui £ 2.000.000 per onorari.

Roma, 7 novembre 2000.

Depositata in Cancelleria il 6 dicembre 2000.

Parte III

PARTE III

RAPPORTI FRA PRIVACY E POSTA ELETTRONICA

In questa sezione sono state brevemente analizzate le problematiche giuridiche relative all'utilizzo della posta elettronica, con particolare attenzione ai riflessi sulla disciplina della riservatezza dei dati personali e al fenomeno dell'invio non richiesto di messaggi pubblicitari, cd. spamming. Inoltre, si è affrontato l'argomento della videosorveglianza posto che molteplici aspetti di tale sistema di controllo sono connessi alla disciplina della protezione dei dati personali.

Partendo dall'analisi del valore giuridico della posta elettronica si può affermare che, nel nostro ordinamento, la violazione della riservatezza di una e-mail corrisponde sostanzialmente alla violazione della corrispondenza in generale, come contenuta nella Carta costituzionale all'art. 15 (la libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili). Inoltre, la riservatezza della corrispondenza è tutelata anche dal codice penale, nel quale, all'art. 616 c.p., si è operata una parificazione tra corrispondenza "epistolare, telegrafica o telefonica, informatica o telematica" [1]*. Non esiste, pertanto, nell'ordinamento italiano una apprezzabile differenziazione tra riservatezza epistolare e telematica. Tuttavia per quanto riguarda, più nello specifico, l'utilizzo della posta aziendale a fini privati è utile ricordare l'ordinanza emessa dal Tribunale di Milano il 10 maggio 2002: in quel caso il Giudice adito ritenne non punibile la lettura da parte del datore di lavoro di alcune e-mail aziendali che avevano portato al licenziamento della lavoratrice. Secondo quell'ordinanza la casella aziendale di posta elettronica andrebbe considerata come un qualsiasi strumento di lavoro e come tale potrebbe essere soggetta al legittimo controllo dell'azienda. E' bene però precisare che, nel caso di specie, si trattava, della lettura di un account aziendale e non di un account privato.*

[1] Sezione V - Dei delitti contro la inviolabilità dei segreti - art. 616 c.p. Violazione, sottrazione e soppressione di corrispondenza - Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da trenta euro a cinquecentosedici euro. Se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni. Il delitto è punibile a querela della persona offesa. Agli effetti delle disposizioni di questa sezione, per «corrispondenza» s'intende quella epistolare, telegrafica o telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza

A tal proposito emerge un ulteriore quesito relativo alla possibilità, per il datore di lavoro, di controllare a distanza il lavoratore. Al caso è applicabile l'art.114 del Codice della privacy (D. Lgs. 196/2003). Questo articolo regolamenta il controllo a distanza dei lavoratori rimandando a quanto disposto dall'art. 4 della legge 20 maggio 1970 n. 300 (il cd. Statuto dei Lavoratori). Secondo tale ultimo articolo, "è vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero alla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna". Quindi il controllo della posta elettronica del dipendente (così come dei file di log di un pc aziendale) si rende possibile quando non è esclusivamente finalizzato al controllo della attività lavorativa, ma è giustificato da "esigenze organizzative e produttive ovvero dalla sicurezza del lavoro", previo accordo o regolamento aziendale.

Per quanto riguarda la seconda problematica affrontata in questa sezione, relativa all'invio di messaggi pubblicitari non richiesti mediante l'utilizzo della posta elettronica, occorre ricordare la posizione del Garante per la protezione dei dati personali che ha sempre mantenuto una linea poco tollerante nei confronti dello spamming, anche prima dell'approvazione della direttiva 2002/58/CE e dell'entrata in vigore del Codice privacy, normative che hanno con maggior chiarezza definito l'illiceità di tale pratica.

Nei primi mesi del 2001, con la decisione dell'11 gennaio (pubblicata nel bollettino del Garante n. 16/2001), il Garante ha ritenuto che gli indirizzi e-mail presenti in internet non fossero assimilabili ai dati personali provenienti da «pubblici registri, elenchi, atti o documenti conoscibili da chiunque» e quindi trattabili anche in assenza del consenso dell'interessato.

Secondo il Garante non è sufficiente che gli indirizzi di posta elettronica vengano lasciati dagli utenti in luoghi accessibili a chiunque (come internet) perché possano dirsi liberamente utilizzabili. Sulla scorta della lettura dell'art. 12 della legge n. 675/96 fornita dal Garante (norma che disciplinava i casi in cui era possibile procedere ad un trattamento di dati in assenza del consenso dell'interessato perché i

trattasi di dati provenienti da elenchi pubblici o registri accessibili da chiunque e per altre tipologie o modalità individuate dal legislatore) non era sufficiente la piena conoscibilità di un dato per renderlo liberamente trattabile, bensì era necessaria l'esistenza di un regime giuridico di piena conoscibilità di quel dato da parte di chiunque (la decisione è consultabile sul sito interlex.it al link http://interlex.it/testi/d010111.htm).

L'attenzione del Garante verso la posta elettronica è comunque, ancora più risalente. Già con la newsletter n. 14/18.7.99 e con il comunicato dal 12 luglio 1999 l'autorità sosteneva che « I messaggi che circolano via e-mail e nelle newsgroup sono da considerare corrispondenza e come tali non possono venire violati».

Nel 2002 il Garante interveniva espressamente sul tema spamming affermando che «è illegittimo utilizzare a scopi commerciali un indirizzo e-mail, che non compare in elenchi pubblici, senza il consenso del destinatario (caso di un fornitore di servizi su Internet, che inviava messaggi pubblicitari non richiesti tramite posta elettronica)»[2]

Nello stesso anno (con la NL 24/30.6.02) il Garante ribadiva che «la presenza dell' indirizzo e-mail di una persona su un sito Internet non autorizza le aziende, per il solo fatto di essere pubblico, ad utilizzarlo per inviare pubblicità», mentre l'anno successivo esprimeva anologhi convincimenti circa l'SMS spamming ammonendo «non è consentito l'invio sul telefonino dell'utente di SMS promozionali, relativi a servizi offerti dalla società gestore di telefonia mobile, senza l'espresso consenso a ricevere questo tipo di informazioni» (NL 3/9.2.03). Sempre in tema di SMS con il parere del 10.6.03 il Garante ha chiarito che «è illecito inviare SMS pubblicitari senza aver prima acquisito il consenso libero ed informato dell'abbonato. Parimenti illecito l'"espediente", adottato da alcuni fornitori di servizi telefonici, di subordinare la stipula del contratto o l'attivazione della carta prepagata alla prestazione del consenso a ricevere messaggi pubblicitari, o quello di inserire tra gli obblighi contrattuali una dichiarazione standard di "impegno" all'invio di SMS commerciali. Il gestore non può "nascondere" comunicazioni commerciali dietro fittizi "messaggi di servizio" alla propria utenza e deve acquisire in ogni caso il consenso libero del destinatario, sia se pubblicizza un servizio "altrui", sia se promuove un servizio della propria società».

[2] *v. Newsletter 13/19.5.02.*

Fra il 2002 ed il 2003 si registrano numerosi interventi del Garante in tema di spamming, come ad esempio la NL 10/16.2.03 e le due decisioni del 25.6.02 e del 25.7.02, ove è stato ulteriormente ribadito che «gli indirizzi di posta elettronica non sono liberamente utilizzabili da chiunque per il solo fatto di trovarsi in rete. La vasta conoscibilità degli indirizzi e-mail che Internet consente non rende lecito l'uso di questi dati personali per scopi diversi da quelli per i quali sono presenti on line. Gli indirizzi e-mail non sono, quindi, "pubblici" come possono essere quelli presenti sugli elenchi telefonici».

Sempre nel 2003 il Garante interveniva con un provvedimento ad hoc sullo spamming, per la precisione il parere del 29 maggio del 2003, in cui ricordava che «gli indirizzi di posta elettronica recano dati di carattere personale da trattare nel rispetto della normativa in materia (art. 1, comma 1 lett. c), legge n. 675). La loro utilizzazione per scopi promozionali e pubblicitari è possibile solo se il soggetto cui riferiscono i dati ha manifestato in precedenza un consenso libero, specifico e informato. Il consenso è necessario anche quando gli indirizzi sono formati ed utilizzati automaticamente con un software senza l'intervento di un operatore, o in mancanza di una previa verifica della loro attuale attivazione o dell'identità del destinatario del messaggio, e anche quando gli indirizzi non sono registrati dopo l'invio dei messaggi. Questo assetto, basato su una scelta dell'interessato c.d. di opt-in, è stato ribadito nel 1998 (con il d.lg. n. 171) prima ancora che una recente direttiva comunitaria lo estendesse a tutti i Paesi dell'Unione europea (n. 2002/58/CE in fase di recepimento in Italia, pubblicata sulla G.U.C.E. n. L 201 del 31 luglio 2002)».

Queste indicazioni del Garante sono state poi ribadite nel Comunicato del 3 settembre del 2003 e nella NL 1-7.09.2003, precisando che «inviare e-mail pubblicitarie senza il consenso del destinatario è vietato dalla legge. Se questa attività, specie se sistematica, è effettuata a fini di profitto si viola anche una norma penale e il fatto può essere denunciato all'autorità giudiziaria».

Nel 2004 il Garante (NL 2-8.02.2004) ha diffuso i risultati di un sondaggio effettuato fra settembre e dicembre 2003, che ha riguardato 21.102 persone di 36 diversi Paesi in tema di spamming. Il sondaggio è stato realizzato dalla TransAtlantic Consumer Dialogue (TACD), un organismo che riunisce 65 associazioni per la tutela dei consumatori in Europa e negli USA, e reso pubblico in occasione della recente

conferenza OCSE sullo spam tenuta il 2-3 febbraio scorsi. Dal sondaggio è emerso che «più della metà dei consumatori rinuncia a servirsi degli strumenti offerti dal commercio elettronico per timore di ricevere spam, e oltre l'80% chiede ai governi di imporre il consenso preventivo (opt-in) per l'invio di messaggi commerciali». Dalle rilevazioni condotte si evinceva il seguente scenario: «i consumatori hanno indicato chiaramente di considerare lo spam un grave elemento di disturbo (96%), e addirittura l'84% ha chiesto di vietarlo espressamente per legge. E' significativo che tali percentuali non varino in misura importante nei 36 Paesi presi in considerazione (…) soprattutto degna di nota è la netta preferenza accordata al consenso preventivo (opt-in) quale approccio da seguire per tutte le comunicazioni commerciali (82%), e all'uso di etichette per segnalare la natura del messaggio in arrivo (ad esempio: ADV per "Advertisement" nel campo "Oggetto" dei messaggi di posta elettronica); l'80% ha indicato di gradire tale soluzione». In conclusione, base quanto riporta il TACD lo spamming costituirebbe un freno allo sviluppo del commercio elettronico.

Il tema dello spamming è stato affrontato anche dall'autorità Garante per la Concorrenza ed il Mercato (AGCOM, meglio nota come Antitrust), con riferimento all'invio di materiale pubblicitario da parte degli Intenet service provider.

In particolare l'antitrust ha evidenziato l'illegittimità dello spamming a fronte della fornitura di determinati servizi presentati come gratuiti. Con diverse pronunce risalenti al 2002 l'autorità ha ricordato come l'invio di materiali pubblicitario e la relativa profilazione dell'utente come corrispettivo della fornitura di un servizio di posta elettronica prefiguri un vera e propria prestazione passiva a carico dell'utente, pertanto la pratica invalsa fra numerosi operatori di pubblicizzazione della prestazione di tali servizi come "gratuita" si appalesa illecita ed ingannevole.

Infine per quanto riguarda l'ultima problematica affrontata in questa sezione è la videosorveglianza in quanto tale attività ha numerosi riflessi sulla disciplina della tutela dei dati personali. Infatti questi sistemi trattano dati personali: la voce e l'immagine, infatti, sono da considerarsi, in base alla Direttiva 95/46/CE ed alla normativa italiana, informazioni riferite ad una persona identificata o identificabile.
Le dimensioni assunte dal fenomeno, specie negli ultimi anni, e le problematiche che l'utilizzo di nuove tecnologie solleva, hanno spinto il Garante ad intervenire per

individuare un punto di equilibrio tra esigenze di sicurezza, prevenzione e repressione dei reati, e diritto alla riservatezza e libertà delle persone.

Nel luglio del 2000 è stata portata a termine la prima indagine sulla presenza di telecamere visibili in Italia.

Prima del provvedimento generale del 29 aprile 2004, il Garante aveva già adottato nel novembre 2000 delle prime linee guida che indicavano le regole per garantire che l'installazione di dispositivi per la videosorveglianza rispetti le norme sulla privacy e sulla tutela della libertà delle persone, in particolare assicurando la proporzionalità tra mezzi impiegati e fini perseguiti.

Il Garante ha, inoltre, avviato le procedure per l'adozione di un codice deontologico e di buona condotta del settore che fissi regole precise e garanzie riguardo alla raccolta, all'uso e alla conservazione delle immagini rilevate attraverso videosorveglianza.

Un intervento del Garante sul rispetto della privacy nell'uso della videosorveglianza da parte delle pubbliche amministrazioni.

NUMERO SCHEDA: 6058

CLASSIFICAZIONE: ATTIVITA' E ATTI AMMINISTRATIVI

SOTTOCLASSIFICAZIONE: Privacy

FONTE: ITALIA OGGI

DATA: 10/03/2005

PAGINA: 33

Con un provvedimento riportato sulla newsletter n. 245 del 2005, il Garante per la privacy è intervenuto in materia di utilizzo di impianti di videosorveglianza ad opera delle pubbliche amministrazioni. Presupposto giuridico dell'intervento, nonché fonte regolatrice della materia, è il provvedimento generale sulla videosorveglianza del 29 aprile 2004 e in particolare la parte in cui viene dettagliato il principio di proporzionalità degli strumenti impiegati rispetto agli obiettivi perseguiti.
Ne emerge che il rispetto di regolamenti amministrativi non legittima l'adozione di trattamenti di videosorveglianza, la quale è lecita solo quando viene garantita l'osservanza del suddetto principio, sia nella scelta preliminare in merito alla necessità di procedere all'installazione di apparecchiature di ripresa, sia in ogni fase successiva o modalità del trattamento.
Pertanto, non rileva tanto l'idoneità dello strumento impiegato rispetto allo scopo quanto la proporzionalità del mezzo rispetto alle finalità, dal momento che risultano coinvolti diritti e interessi dei cittadini costituzionalmente tutelati, considerati prevalenti rispetto ad un altro principio generale, anch'esso costituzionalizzato: quello del buon andamento della pubblica amministrazione.

Si riporta il testo dell'intervento del Garante in esame.

Videosorveglianza: nuovi interventi del Garante

Tolte le telecamere per controllare lo smaltimento dei rifiuti e modificate quelle davanti ad un centro medico
Nuovi interventi del Garante contro i sistemi di videosorveglianza illeciti. Accolto il ricorso di un dentista che temeva per la privacy dei suoi pazienti ripresi dalle telecamere di un laboratorio attiguo e disattivato un impianto comunale installato in un'area adibita allo smaltimento dei rifiuti.
Nel primo caso il Garante, accogliendo il ricorso di un centro medico dentistico, il cui ingresso era ripreso dalle telecamere di un laboratorio odontotecnico contiguo, ha stabilito che le riprese sono lecite solo se vengono limitate all'area direttamente interessata dalle esigenze di sicurezza. Inoltre, chi si trova a passare deve essere opportunamente avvertito della presenza dell'impianto. Dopo un primo intervento dell'Autorità che lo invitava ad aderire spontaneamente alle richieste del ricorrente, il titolare del laboratorio ha sostenuto che l'installazione dell'impianto si era resa necessaria dopo il ripetersi di atti vandalici, avvenuti di solito dopo gli orari di chiusura; che la conservazione delle riprese era di brevissima durata e le immagini potevano essere visionate, con l'ausilio di un tecnico, solo in caso di ulteriori episodi. Giustificazioni risultate insufficienti: il Garante ha ritenuto illecito e non conforme al principio di proporzionalità il trattamento delle immagini che "spaziano" nell'ingresso del vicino centro medico, stabilendo che il laboratorio dovrà correggere l'angolo di ripresa e collocare adeguati cartelli informativi.

Nel secondo caso un'associazione di risparmiatori e consumatori si è rivolta all'Autorità segnalando l'installazione delle telecamere da parte di un comune che intendeva monitorare le operazioni di smaltimento dei rifiuti per verificare che venissero rispettate le disposizioni sulla raccolta differenziata. L'Ufficio del Garante, nel richiamare l'ente locale al rispetto del Codice in materia di protezione dei dati personali e, in particolare, alle indicazioni fornite dal Garante nel provvedimento generale del 29 aprile 2004, ha ricordato che non è lecito utilizzare sistemi di videosorveglianza solo per accertare eventuali violazioni amministrative derivanti dal mancato rispetto delle disposizioni su modalità e orari di deposito dei sacchetti dei rifiuti dentro gli appositi contenitori. Il Comune, quindi, invitato a conformarsi alle citate prescrizioni, ha comunicato di aver disattivato l'impianto e di aver cancellato tutte le immagini registrate.

Articolo sulla tutela della riservatezza nel nuovo codice in materia di protezione di dati personali.

NUMERO SCHEDA: 5108

FONTE: GIUSTIZIA CIVILE

AUTORE: Roberta Montinaro

NUMERO: 5

DATA: 01/05/2004

PAGINA: 247-267

NATURA ATTO: COMMENTO

E' disponibile presso il Settore Studi e Documentazioni un articolo di Roberta Montinaro dal titolo: *Tutela della riservatezza e risarcimento del danno nel nuovo codice in materia di protezione dei dati personali.*
In esso l'autrice, dopo aver fatto una breve storia della normativa in materia di protezione di dati personali in Italia, pone il diritto alla protezione dei dati in raffronto con l'ingiustizia del danno.
Inoltre, parlando del rapporto tra problema della protezione dei dati e diritto alla riservatezza, analizza anche la questione del risarcimento dei danni non patrimoniali.

Il Garante per la protezione dei dati personali interviene contro l'uso indiscriminato dei sistemi di rilevazione delle impronte digitali da parte delle pubbliche amministrazioni.

NUMERO SCHEDA: 4291

CLASSIFICAZIONE: ATTIVITA' E ATTI AMMINISTRATIVI

SOTTOCLASSIFICAZIONE:

FONTE: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DATA: 18/01/2004

RIFERIMENTO NORMATIVO:

NATURA ATTO: COMUNICAZIONE

DATA ATTO: 18/01/2004

Il Garante per la protezione dei dati personali ha adottato una posizione critica nei confronti dell'uso indiscriminato dei sistemi di rilevazione delle impronte digitali da parte delle amministrazioni pubbliche quando questo tipo di operazione risulta sproporzionata agli scopi che si intendono perseguire, in considerazione della particolare delicatezza del trattamento di dati personali ipotizzato.
Come informa la newsletter del 18 gennaio 2004 il Garante ha reso noto i risultati delle 56 ispezioni (30 in più rispetto al 2002) che l'Ufficio del Garante, a cura del Dipartimento vigilanza e controllo, ha effettuato nel corso del 2003.
Gli accertamenti condotti dal Garante riguardano i sistemi di controllo degli accessi degli studenti in una mensa universitaria e dei dipendenti in una biblioteca comunale.
Secondo il Garante occorre evitare l'utilizzo di strumenti sproporzionati agli scopi che si intende perseguire e di prevedere rigorose cautele.
In particolare, nei casi di specie, gli enti interessati dall'accertamento dovranno fornire ogni elemento o documento che permetta di valutare le caratteristiche del progetto, precisando per quali motivi non sarebbero idonei altri sistemi o procedure che creano minori pericoli o rischi per i diritti e le libertà fondamentali di chi deve rilasciare le impronte ed indicare le finalità perseguite nell'utilizzare tali sistemi di rilevazione, e specificando le modalità di registrazione del dato biometrico ed il successivo confronto dell'impronta digitale registrata con quella rilevata dai lettori ottici, ed indicare periodo di conservazione dei dati personali, misure di sicurezza adottate e modalità di consultazione della banca dati da parte di soggetti autorizzati.

Si allega il testo della newsletter.

Garante per la protezione dei dati personali
Newsletter
Notiziario settimanale. Anno V n. 197 (12 - 18 gennaio 2004)
Impronte digitali in mensa e in biblioteca Il Garante interviene contro l'uso indiscriminato da parte delle pubbliche amministrazioni
Stop del Garante all'uso indiscriminato dei sistemi di rilevazione delle impronte digitali da parte delle amministrazioni pubbliche. Occasione per la presa di posizione due casi, uno relativo al controllo degli accessi degli studenti in una mensa universitaria e l'altro riguardante il controllo dei dipendenti in una biblioteca comunale, per i quali l'Autorità (Stefano Rodotà, Giuseppe Santaniello, Gaetano Rasi, Mauro Paissan), fin dall'inizio del procedimento, ha già ribadito la necessità di evitare l'utilizzo di strumenti sproporzionati agli scopi che si intende perseguire e di prevedere rigorose cautele.
Nel primo caso, gli accertamenti sono stati avviati nei confronti di un ente regionale per il diritto allo studio universitario, che, secondo notizie di stampa, era in procinto di bandire una gara di appalto per installare lettori di impronte digitali in ristoranti e pizzerie convenzionati per controllare che l'accesso al servizio di ristorazione avvenisse esclusivamente da parte degli aventi diritto (studenti vincitori di borse di studio o in particolari condizioni di reddito, studenti apolidi, etc.). Ciò perché vi è il sospetto che i ticket siano ceduti e utilizzati da chi non ne ha diritto, con danno per l'ente che partecipa alla spesa dei pasti.
Nel secondo caso, gli accertamenti riguardano un comune che avrebbe invitato tutti i dipendenti, ed in particolare quelli in servizio presso la biblioteca comunale, a depositare le proprie impronte digitali per costituire addirittura una banca dati da utilizzare per la rilevazione delle presenze.
I due procedimenti, che verranno definiti in breve tempo, si sono resi necessari in considerazione della particolare delicatezza del trattamento di dati personali ipotizzato, cioè la raccolta e l'uso delle impronte

digitali. Trattamento che deve essere effettuato nel rispetto di precise garanzie in materia di tutela della privacy.
Il Garante intende, anzitutto, accertare se l'uso di un sistema così invasivo come quello di rilevazione delle impronte digitali sia, come previsto dalla normativa sulla privacy, proporzionato alla finalità che si vuole perseguire, ossia di consentire l'accesso al servizio di mensa universitaria, di controllare l'orario di servizio dei dipendenti o l'accesso alla biblioteca comunale da parte degli aventi diritto. Entro trenta giorni l'ente universitario e il comune dovranno fornire al Garante ogni elemento o documento che permetta di valutare le caratteristiche del progetto. Dovranno precisare, tra l'altro, per quali motivi non sarebbero idonei altri sistemi o procedure che creano minori pericoli o rischi per i diritti e le libertà fondamentali di chi deve rilasciare le impronte ed indicare le finalità perseguite nell'utilizzare tali sistemi di rilevazione. I due enti dovranno altresì specificare le modalità di registrazione del dato biometrico ed il successivo confronto dell'impronta digitale registrata con quella rilevata dai lettori ottici, ed indicare periodo di conservazione dei dati personali, misure di sicurezza adottate e modalità di consultazione della banca dati da parte di soggetti autorizzati.
Nel 2003 quasi triplicate le ispezioni del Garante
Il bilancio di un anno di attività
Nel settore privato aziende più grandi iniziano ad affrontare meglio la legge predisponendo anche "uffici privacy", avvalendosi magari di collaborazioni esterne, mentre aziende medio piccole trascurano di più la materia ed evidenziano un livello inferiore di adeguamento alla normativa e agli indirizzi del Garante. Nella pubblica amministrazione la cultura della privacy stenta ad affermarsi: processi di lavoro e gestione delle pratiche di ufficio poco rispettosi della legge sulla tutela dei dati personali e, in alcuni casi, assoluta noncuranza e superficialità nel trattamento dei dati.
Questo il quadro che emerge dalle 56 ispezioni che l'Ufficio del Garante, a cura del Dipartimento vigilanza e controllo, ha effettuato lo scorso anno nei confronti di pubbliche amministrazioni e privati. Complessivamente 30 in più rispetto al 2002. L'incremento dell'attività ispettiva si è potuto realizzare anche grazie allo stretto rapporto di collaborazione con la Guardia di finanza stabilito con il protocollo siglato nell'ottobre 2002, che prevede uno stretto rapporto con il Comando Unità speciali del Corpo.
I controlli sono stati originati da segnalazioni di cittadini o di organi di stampa (48%), che hanno reso necessaria una verifica sul posto e da ricorsi (42%), dai quali sono emersi profili che meritavano accertamenti autonomi. Cicli di ispezioni e controlli incrociati, pari al 10% del totale, sono stati effettuati d'ufficio per verificare il rispetto della normativa in determinati settori.
Le ispezioni hanno riguardato nel 34% dei casi le modalità di acquisizione del consenso, soprattutto nell'ambito delle comunicazioni commerciali indesiderate via Internet e nel 26% il rispetto della normativa in materia di videosorveglianza.
In un ulteriore 26% dei casi l'ispezione ha accertato l'origine dei dati personali trattati mentre nel 12% ha verificato le misure di sicurezza. Gli interventi recenti sono stati effettuati su tutta la penisola, anche se in questa fase si sono concentrati nelle regioni settentrionali e centrali dove sono localizzate in prevalenza le aziende private controllate. Nel corso delle attività ispettive sono state accertate numerose violazioni amministrative e, nel 10% dei casi, si è proceduto ad inviare segnalazioni all'Autorità giudiziaria per violazioni costituenti reato quali: il trattamento illecito di dati personali, la mancata adozione delle misure di sicurezza, l'inottemperanza ai provvedimenti del Garante.
Alcune ispezioni hanno consentito inoltre di portare alla luce gravi inadempienze per l'accertamento delle quali sono state avviate complesse indagini di polizia giudiziaria ancora in corso.
L'esperienza ha evidenziato anche un buon rapporto istituzionale con i presidenti dei tribunali competenti per il territorio che, nei casi in cui occorreva una loro autorizzazione, hanno accolto tempestivamente con provvedimenti motivati le richieste dell'Autorità.
Per quanto riguarda il futuro, pubblica amministrazione, Internet, trattamento informatico dei dati saranno i settori sui quali maggiormente si concentrerà l'attività ispettiva del Garante Privacy. All'inizio dell'anno 2004 è stato rafforzato il rapporto di collaborazione con la Guardia di finanza, con l'obiettivo di incrementare ancora l'efficacia dell'attività di controllo dell'Autorità

Un provvedimento del Garante per la protezione dei dati personali impone l'identificazione del mittente nei messaggi commerciali.

NUMERO SCHEDA: 3723

CLASSIFICAZIONE: ATTIVITA' E ATTI AMMINISTRATIVI

FONTE: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NATURA ATTO: PROVVEDIMENTO

Il provvedimento del Garante per la protezione dei dati personali, qui segnalato, affermando che l'invio anonimo di messaggi pubblicitari senza l'identificazione di un mittente costituisce un caso di trattamento illecito dei dati personali anticipa il recepimento della direttiva europea 2002/58/Ce. Infatti già dalla disciplina contenuta nella l. 675/1996 e nel d.lgs. 171/1998 si desume l'obbligo, a carico del mittente del messaggio elettronico, di indicare il suo indirizzo fisico ove il destinatario può esercitare i diritti attribuiti dalla legge 675/1996.

Si riporta qui di seguito il testo integrale del provvedimento, già riportato a pg. 397.

PREMESSO:

1. I DISAGI DI NUMEROSI UTENTI

Continuano a pervenire a questa Autorità diverse centinaia di reclami e segnalazioni da parte di utenti di reti telematiche e di associazioni per la tutela dei diritti di utenti e consumatori, che contestano la ricezione di messaggi di posta elettronica per scopi promozionali, pubblicitari, di informazione commerciale o di vendita diretta, inviati senza che gli interessati abbiano manifestato in precedenza il proprio consenso informato.

Numerosi interessati espongono anche ulteriori disagi derivanti dalla costante ripetizione di analoghi messaggi da parte di uno stesso mittente titolare del trattamento, dai vani tentativi esperiti per ottenere sia la cancellazione del proprio indirizzo di posta elettronica presso i mittenti, sia l'interruzione di altri messaggi. Altre segnalazioni riguardano gli inconvenienti che derivano dalla ricezione di e-mail anonime o prive dell'indicazione di un indirizzo, oppure delle coordinate veritiere di un reale mittente.

Nella prevalenza dei casi, agli interessati non è stato previamente richiesto, come dovuto, uno specifico consenso preceduto da un'idonea informativa che illustri adeguatamente le modalità e le caratteristiche dei messaggi.

In altri casi i messaggi sono inviati da imprese -anche in questo caso senza consenso- per promuovere, presso clienti, prodotti o servizi analoghi a quelli forniti in un rapporto contrattuale, oppure per offrire altri tipi di prodotti o servizi distribuiti anche da terzi.

Il Garante ha fornito assistenza a numerosi cittadini, indicando le opportune modalità di tutela; ha poi attivamente cooperato in sede comunitaria per l'adozione di decisioni comuni alle autorità di garanzia dei Paesi dell'Unione europea, pubblicate nel sito Internet di quest'ultima e in quello del Garante (www.garanteprivacy.it).

L'Autorità ha anche accolto numerosi ricorsi (art. 29 legge n. 675/1996), a seguito dei quali sono stati impartiti specifici divieti di trattamento dei dati. Sono stati altresì avviati i procedimenti per applicare le pertinenti sanzioni amministrative e sono stati trasmessi gli atti all'autorità giudiziaria penale nei casi in cui erano configurabili reati.

Con la collaborazione di forze di polizia, incaricate da questa Autorità di svolgere i necessari controlli e di dare esecuzione ai provvedimenti, sono stati eseguiti in loco, presso fornitori di servizi ed altri titolari di trattamento, vari provvedimenti di sospensione temporanea di ogni operazione illecita del trattamento dei dati personali da parte di società risultate responsabili di attività svolte in modo sistematico. Infine, sono stati eseguiti accertamenti presso altri fornitori di servizi di accesso ad Internet o ulteriori soggetti, per verificare la rispondenza dei trattamenti di dati alla normativa vigente.

A conclusione di queste attività, il Garante ravvisa la necessità di adottare un provvedimento di carattere generale per indicare le misure che gli operatori del settore devono adottare al fine di conformarsi alla disciplina generale sull'uso dei dati personali, specie nel settore delle comunicazioni (in particolare, alla legge 31 dicembre 1996, n. 675, al decreto legislativo 13 maggio 1998, n. 171 e al decreto legislativo 22 maggio 1999, n. 185). L'Autorità ritiene inoltre necessario inibire il trattamento illecito di dati risultante da altre segnalazioni il cui esame è stato riunito in un unico procedimento, in particolare di quelle relative a titolari di trattamento identificabili.

2. INVIO LECITO DI POSTA ELETTRONICA PUBBLICITARIA

Gli indirizzi di posta elettronica recano dati di carattere personale da trattare nel rispetto della normativa in materia (art. 1, comma 1 lett. c), legge n. 675).

La loro utilizzazione per scopi promozionali e pubblicitari è possibile solo se il soggetto cui riferiscono i dati ha manifestato in precedenza un consenso libero, specifico e informato.

Il consenso è necessario anche quando gli indirizzi sono formati ed utilizzati automaticamente con un software senza l'intervento di un operatore, o in mancanza di una previa verifica della loro attuale attivazione o dell'identità del destinatario del messaggio, e anche quando gli indirizzi non sono registrati dopo l'invio dei messaggi.

Questo assetto, basato su una scelta dell'interessato c.d. di opt-in, è stato ribadito nel 1998 (con il d.lg. n. 171) prima ancora che una recente direttiva comunitaria lo estendesse a tutti i Paesi dell'Unione europea (n. 2002/58/CE in fase di recepimento in Italia, pubblicata sulla G.U.C.E. n. L 201 del 31 luglio 2002).

Questa Autorità si è pronunciata più volte in materia ribadendo che la circostanza che gli indirizzi di posta elettronica possano essere reperiti con una certa facilità in Internet non comporta il diritto di utilizzarli liberamente per inviare messaggi pubblicitari (cfr., ra l'altro, la decisione dell'11 gennaio 2001 - in Bollettino del Garante n. 16).

In particolare, i dati dei singoli utenti che prendono parte a gruppi di discussione in Internet sono resi conoscibili in rete per le sole finalità di partecipazione ad una determinata discussione e non possono essere utilizzati per fini diversi qualora manchi un consenso specifico (art. 9, comma 1, lettere a) e b), legge n. 675).

Ad analoga conclusione deve pervenirsi per gli indirizzi di posta elettronica compresi nella lista "anagrafica" degli abbonati ad un Internet provider (qualora manchi, anche in questo caso, un consenso libero e specifico), oppure pubblicati su siti web di soggetti pubblici per fini istituzionali.

Tali considerazioni valgono anche con riferimento ai messaggi pubblicitari inviati a gestori di siti web - anche di soggetti privati- utilizzando gli indirizzi pubblicati sugli stessi siti, o che sono reperibili consultando gli elenchi dei soggetti che hanno registrato i nomi a dominio. In quest'ultimo caso, infatti, la conoscibilità in rete degli indirizzi è volta a identificare il soggetto che è o appare responsabile, sul piano tecnico o amministrativo, di un nome a dominio o di altre funzioni rispetto a servizi Internet (per la tutela di vari diritti sul piano civile e penale, anche ai sensi della legge n. 675) e non anche a rendere l'interessato disponibile all'invio di messaggi pubblicitari).

In tutti questi casi, l'utilizzo spesso massivo della posta elettronica comporta una lesione ingiustificata dei diritti dei destinatari, costretti ad impiegare diverso tempo per mantenere un collegamento e per ricevere, come pure per esaminare e selezionare, tra i diversi messaggi ricevuti, quelli attesi o ricevibili, nonché a sostenere i correlativi costi per il collegamento telefonico (incrementati anche da messaggi di dimensioni rilevanti che rallentano tali operazioni), oppure ad adottare "filtri", a verificare più attentamente la presenza di virus, o a cancellare rapidamente materiali inadatti a minori specie in ambito domestico.

Il fenomeno interessa anche piccole e grandi imprese destinatarie di un elevato numero di messaggi, le quali devono farsi carico di misure interne e di costi anche organizzativi per contrastarlo.

Questo ingiustificato riversamento sugli utenti dei costi pubblicitari si verifica anche relativamente a messaggi inviati da singole persone fisiche che, in vari casi esaminati, non si limitano ad una comunicazione episodica, ma intraprendono una comunicazione sistematica per fini personali o, addirittura, una diffusione di dati cui è applicabile la disciplina in materia di protezione dei dati personali (art. 3 legge n. 675).

3. IL QUADRO GIURIDICO SU INFORMATIVA E CONSENSO

La legge individua il contenuto dell'informativa agli interessati, nonché i casi in cui è necessario il consenso espresso dell'interessato o è possibile prescinderne (artt. 10, 11, 12 e 20 legge n. 675).

Al riguardo va nuovamente rilevato che non può farsi a meno del consenso ritenendo che i dati personali relativi all'indirizzo di posta elettronica –e all'indirizzo in particolare- siano "pubblici" in quanto conoscibili da chiunque.

Le disposizioni normative che si riferiscono a questo aspetto (artt. 12, comma 1, lett. c) e 20, comma 1, lett. b) legge cit.) sono infatti applicabili solo quando vi è un pubblico registro, elenco, atto o documento conoscibile da chiunque perché vi è una specifica disciplina che ne impone la conoscibilità indifferenziata da parte del pubblico, e non anche quando i dati personali sono conoscibili da chiunque per mere circostanze di fatto (si pensi, oltre ai casi già richiamati di raccolta su siti web o di messaggi trasmessi su newsgroup o su mailing list, agli indirizzi di posta elettronica raccolti in rete tramite appositi software o mediante comuni motori di ricerca).
Il principio del consenso è quindi già operante nel nostro ordinamento prima ancora di essere affermato senza eccezioni su scala europea, dalla menzionata direttiva n. 2002/58 in fase di recepimento, a tutta la posta elettronica comunque inviata per fini di commercializzazione diretta (si vedano in particolare l'art. 13 e il considerando n. 40).
Il quadro evidenziato trova conferma nella disciplina sulla protezione dei consumatori nei contratti a distanza che, in riferimento al rapporto sottostante ai fini del quale si procede al trattamento di dati personali, vieta ai fornitori l'impiego della posta elettronica in mancanza del consenso preventivo del consumatore, in relazione a determinati scopi tra i quali rientrano anche quelli pubblicitari (art. 10, comma 1, d.lg. 22 maggio 1999, n. 185).
Per gli aspetti relativi alla protezione dei dati personali non devono essere peraltro considerate le disposizioni del recente decreto legislativo 9 aprile 2003, n. 70, sul commercio elettronico, dichiarate in proposito espressamente inapplicabili (art. 1, comma 2, lett. b) d.lg. n. 70 cit.).
Il consenso, da documentare per iscritto, deve essere manifestato liberamente, in modo esplicito e in forma differenziata rispetto alle diverse finalità e alle categorie di servizi e prodotti offerti, prima dell'inoltro dei messaggi (art. 11 legge n. 675).
Tale disciplina non può essere elusa inviando una prima e-mail che, nel chiedere un consenso abbia comunque un contenuto promozionale oppure pubblicitario, oppure riconoscendo solo un diritto di tipo c.d. "opt-out" al fine di non ricevere più messaggi dello tesso tenore.
Al contrario, è opportuna e va incoraggiata la prassi di alcuni fornitori i quali, dopo aver ottenuto realmente un valido consenso dei destinatari, danno semplice conferma della sua manifestazione, attraverso un messaggio volto unicamente ad annunciare il successivo inoltro di materiale pubblicitario. Tale prassi, se utilizzata correttamente, consente tra l'altro di verificare l'effettiva corrispondenza dell'indirizzo di posta elettronica ai soggetti che avevano espresso il consenso, nonché di accertare il permanere di tale volontà.
L'insieme dei diritti riconosciuti dalla legge agli utenti determina, in caso di loro violazione, un trattamento illecito dei dati che:

- è già vietato direttamente dalla legge, senza che sia necessario adottare uno specifico provvedimento interdittivo del Garante dell'autorità giudiziaria;- determina, a seconda dei casi, l'applicazione di sanzioni amministrative pecuniarie, in particolare per
- omessa informativa od omessa notificazione (artt. 10, 34 e 39 legge n. 675; art. 12 d.lg. n. 185/1999);
- comporta il rimborso delle spese e dei diritti relativi al procedimento attivato da un fondato ricorso al Garante, oppure da un'azione dinanzi al giudice civile, come pure il risarcimento dei danni, specie di tipo patrimoniale, che derivino dai fatti illeciti e siano comprovati dall'interessato in relazione ai disagi sopra illustrati;
- rende applicabile anche una sanzione penale qualora il trattamento illecito dei dati sia effettuato al fine di trarne per sé o per altri un profitto o per arrecare ad altri un danno, con la pena accessoria della pubblicazione della sentenza di condanna (artt. 35 e 38 legge n. 675).

4. MESSAGGI PUBBLICITARI A PROPRI CLIENTI
Per effetto del recepimento della direttiva 2002/58/CE sarà peraltro possibile integrare, nel prossimo futuro, la disciplina sopra illustrata, permettendo a talune società di far conoscere a propri clienti prodotti o servizi analoghi a quelli per i quali si è già stabilito un rapporto, con i medesimi clienti, di vendita di prodotti o servizi.
In tali casi, la società titolare del trattamento (dopo aver informato preventivamente e adeguatamente il cliente) potrà procedere all'invio del messaggio pubblicitario, offrendo però al cliente, in modo chiaro e distinto (sia al momento della raccolta dei suoi dati, sia in occasione di ciascun messaggio) il diritto di rifiutare sin dall'inizio tale uso dei dati o di obiettare, gratuitamente e in maniera agevole, anche successivamente (art. 13, par. 2, direttiva n. 2002/58/CE cit.)
5. MESSAGGI PER CONTO TERZI E ACQUISTO DI BANCHE DATI
In alcuni casi portati all'attenzione del Garante, l'invio di messaggi pubblicitari era stato effettuato, per

conto di terzi committenti, da società specializzate che utilizzano indirizzi di posta elettronica contenuti in proprie banche dati.
Tali società, da considerarsi "titolari" o contitolari del trattamento dei dati a seconda del rapporto che si instaura con il committente e delle modalità di concreta utilizzazione dei dati, sono tenute a rispettare le disposizioni in tema di informativa e specifico consenso, anche per quanto riguarda l'eventuale comunicazione di dati personali ai committenti medesimi e le relative finalità.
Ciò comporta un quadro di obblighi e possibili responsabilità anche penali che gli operatori devono verificare con attenzione, anche uando la società specializzata incaricata sia stabilita fuori dell'Unione europea.
Dall'esame dei reclami e delle segnalazioni pervenuti al Garante è risultato, altresì, che alcuni dei soggetti che hanno utilizzato la posta elettronica per l'invio di messaggi pubblicitari avevano acquisito da terzi le banche dati contenenti gli indirizzi dei destinatari. In questi casi, chi acquisisce la banca dati deve accertare che ciascun interessato abbia validamente acconsentito alla comunicazione del proprio indirizzo di posta elettronica ed al suo successivo utilizzo ai fini di invio di materiale pubblicitario; al momento in cui registra i dati deve poi inviare in ogni caso, a tutti gli interessati, un messaggio di informativa che precisi gli elementi indicati nell'art. 10 della legge n. 675, comprensivi di un riferimento di luogo -e non solo di posta elettronica- presso cui l'interessato possa esercitare i diritti riconosciuti dalla legge.

6. DIRITTI DEGLI INTERESSATI

Indipendentemente dal rapporto esistente tra i mittenti ed i destinatari dei messaggi, chi detiene i dati deve assicurare in ogni caso agli interessati la possibilità di far valere in ogni momento i diritti riconosciuti dalla legge, i quali sono spesso esercitati per conoscere da quale fonte sono stati tratti i dati, o per far interrompere gratuitamente la loro ulteriore utilizzazione ai fini commerciali-pubblicitari, oppure per far cancellare i dati trattati in violazione di legge (art. 13, comma 1, lett. e), della legge).
Nel sito Internet del Garante è riportato un modello-tipo per esercitare tali diritti in maniera agevole, gratuitamente e senza particolari formalità, anche verbalmente o mediante posta elettronica, dimostrando la propria identità (art. 17, comma 1, d.P.R. n. 501 del 31 marzo 1998). Tale modello è utilizzabile in luogo di altri reperibili in reti telematiche che non sono pienamente validi in quanto si riferiscono anche ad aspetti non riconosciuti dall'art. 13 della legge n. 675 (ad esempio, chiedono il rilascio di attestazioni o la copia di autorizzazioni non previste).
I diritti vanno esercitati sulla base di tale modello direttamente presso l'indirizzo conoscibile del titolare o del responsabile del trattamento, riservando solo ad un'eventuale momento successivo l'instaurazione di una procedura contenziosa dinanzi al Garante o all'autorità giudiziaria.
Anche ai fini dell'esercizio di tali diritti, deve ritenersi che l'invio anonimo di messaggi pubblicitari senza l'indicazione di un mittente identificabile concreti già oggi un trattamento illecito di dati personali, a prescindere da quanto dispone il citato d.lg. n. 70/2003 sul commercio elettronico (come si è visto, fuori della materia della protezione dei dati personali) e da quanto, in riferimento ai dati personali, sarà previsto con il recepimento della direttiva n. 2002/58/CE (la quale non consente l'invio di messaggi pubblicitari quando l'identità del mittente viene camuffata o addirittura celata e quando non viene fornito un indirizzo valido che consenta al destinatario di richiedere la cessazione delle comunicazioni: art. 13, par. 4, dir. cit.).
I mittenti dei messaggi devono quindi indicare già oggi, in modo chiaro, la fonte di provenienza del messaggio, nonché il soggetto e l'indirizzo –non solo di posta elettronica- presso cui i destinatari possono esercitare i propri diritti (si veda, in proposito, l'art. 10, comma 1, lett. f) della legge n. 675). Appare altresì conforme al principio di correttezza indicare nell'oggetto del messaggio la sua tipologia pubblicitaria-commerciale (art. 9, comma 1, lett. a), legge n. 675).

7. ELENCHI DI POSSIBILI DESTINATARI

L'eventuale elenco predisposto da operatori, contenente i nominativi dei soggetti che non hanno manifestato il consenso o che lo hanno revocato (c.d. black list) non può essere utilizzato per porre a carico degli interessati, anche indirettamente, un onere di iscrizione nell'elenco medesimo.
Come si è illustrato, il consenso ha un connotato autorizzatorio "positivo" in base al quale l'eventuale silenzio dell'interessato omporta il diniego del consenso eventualmente richiesto e non rileva come assenso tacito all'invio dei messaggi.
Consta peraltro che alcuni operatori intendono adottare la diversa prassi di redigere anche tramite siti web appositi elenchi di persone che hanno manifestato il consenso, distinti in base alle diverse categorie di messaggi commerciali-pubblicitari che gli interessati hanno acconsentito a ricevere. Tale prassi, se correttamente seguita, può rappresentare una misura utile, sul piano organizzativo, per garantire un più effettivo rispetto della volontà espressa dai singoli. A tale riguardo, costituirà una pratica utile

quella di garantire agli interessati la possibilità di inserire direttamente il proprio nome nelle diverse liste o di cancellarlo dalle stesse, magari attraverso un'apposita pagina web, ferma restando l'esigenza di identificarli.

8. E-MAIL PROVENIENTI DALL'ESTERO

Ad alcuni messaggi, in quanto provenienti dall'estero, non è applicabile la legge italiana sulla protezione dei dati personali.

Ciò non comporta l'assoluta mancanza di rimedi o tutela, potendo l'utente chiedere una verifica da parte della competente autorità nazionale di protezione dei dati personali, ove istituita nel Paese eventualmente individuabile dal messaggio.

In altri casi, come quelli relativi alle leggi degli stati federali, l'invio di messaggi pubblicitari di posta elettronica può essere illecito in base alla legge di alcuni stati, per cui è parimenti possibile, per gli utenti, chiedere alle competenti autorità pubbliche degli stati di valutare la perseguibilità degli illeciti.

Va infine tenuto presente che alcune e-mail indesiderate possono essere lo strumento per commettere reati comuni (ad esempio di truffa) che devono considerarsi commessi nel territorio italiano quando, sebbene l'azione è avvenuta all'estero, l'evento-reato che ne deriva si è verificato in Italia.

Questa Autorità si riserva di valutare la posizione dei singoli fornitori di servizi i cui trattamenti sono stati oggetto di segnalazione, anche alla luce dell'ulteriore documentazione eventualmente pervenuta.

In questo quadro, con separati provvedimenti relativi all'esame dei singoli reclami e segnalazioni, si provvederà, oltre alle eventuali trasmissioni di atti all'autorità giudiziaria penale:

a) a contestare la violazione amministrativa relativa agli obblighi di informativa di cui all'art. 10 della legge 31 dicembre 1966, n. 675;

b) ad avviare il procedimento per l'applicazione delle ulteriori sanzioni amministrative previste dal d.lg. n. 185/1999;

TUTTO CIÒ PREMESSO IL GARANTE:

- ai sensi dell'art. 31, comma 1, lett. l) della legge 31 dicembre 1996, n. 675, vieta l'ulteriore trattamento illecito di dati personali realizzato a scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva, effettuato in violazione delle disposizioni sopra richiamate da parte dei soggetti cui si riferiscono le segnalazioni e i reclami pervenuti;
- ai sensi dell'art. 31, comma 1, lett. c) della legge 31 dicembre 1996, n. 675, segnala ai titolari del trattamento di cui agli atti del procedimento la necessità di conformare i trattamenti di dati personali ai principi richiamati nel presente provvedimento.

E-government: il punto dei Garanti europei

NUMERO SCHEDA: 3333

CLASSIFICAZIONE: E-GOVERNMENT

FONTE: WWW.GARANTEPRIVACY.IT/GARANTE/NAVIG/JSP/INDEX.JSP

DATA: 15/06/2003

NATURA ATTO: MESSAGGIO

DATA ATTO: 15/06/2003

ORGANO: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

La newsletter del Garante per la protezione dei dati personali del 9- 15 giugno 2003 prende spunto da un documento recentemente approvato dai Garanti europei in cui vengono analizzate la situazione corrente e le prospettive di sviluppo in tema di *e-government*, sottolineandone le interconnessioni con il tema della protezione dei dati personali e con i possibili rischi del mancato coordinamento fra governi nazionali ed autorità di protezione dati.

Tutti i Garanti hanno giudicato positivamente la firma digitale, quale possibile ausilio per offrire una migliore tutela dell'identità personale ed hanno rilevato che, però, l'esperienza risulta limitata: sono pochi i settori nei quali è possibile servirsi della firma digitale, per motivi di vario genere (costi elevati, assenza di norme regolamentari, complessità dei sistemi esistenti).
Hanno inoltre sottolineato che è fondamentale prevedere un'adeguata e chiara informazione degli utenti da parte dei servizi di certificazione (destinatari delle informazioni raccolte, misure di sicurezza etc.).

Si riporta di seguito la newsletter in commento.

(Garante per la protezione dei dati personali: Newsletter, 9 - 15 giugno 2003).

E-government: il punto dei Garanti europei

Bilancio positivo ma è necessario un maggiore coordinamento tra autorità per la privacy e governi nazionali.
In un documento recentemente pubblicato (disponibile all'indirizzo http://www.europa.eu.int/, per il momento soltanto in lingua inglese) i Garanti europei hanno analizzato la situazione corrente e le prospettive di sviluppo in tema di e-government, sottolineandone le implicazioni in chiave di protezione dei dati personali e richiamando l'attenzione sui possibili rischi del mancato coordinamento fra governi nazionali e autorità di protezione dati.
Il documento dei Garanti prende spunto dalle indicazioni del piano di azione "e-Europe" approvato nel giugno 2000 durante il Consiglio europeo di Feira, in Portogallo. In esso lo sviluppo di forme di e-government era citato fra le priorità di intervento dei governi europei, e si forniva anche una lista di 20 procedure che nei prossimi anni dovranno essere disponibili on-line: dalla creazione di "portali" unificati di accesso alla pubblica amministrazione, alla possibilità di effettuare pagamenti online o ottenere certificati e copie di documenti ufficiali, fino all'introduzione di veri e propri "documenti di identità elettronici". Attraverso un questionario diffuso fra tutte le autorità nazionali di protezione dati, si è cercato di capire quale fosse lo stato dell'arte in Europa, quali di queste iniziative fossero già state realizzate o fossero in via di realizzazione, e quali fossero i principali problemi evidenziati dalle autorità nazionali – non sempre consultate così come previsto dalla legislazione interna.
- Un primo punto da sottolineare è proprio l'attenzione non sempre elevata che i governi dei 15 sembrano prestare al tema della protezione dei dati in questo contesto. Per quanto l'obbligo di consultare l'autorità competente sia previsto per legge nella quasi totalità dei Paesi UE (in Italia dall'art. 31(2) della Legge 675/96), la consultazione non appare sistematica. In vari Paesi si è verificato, infatti, che alcune iniziative di e-government siano state attuate senza avere sentito l'autorità nazionale per la protezione dei dati. Tuttavia, il bilancio tratto è sostanzialmente positivo: attraverso consultazioni pubbliche (come in Francia o nel Regno Unito), procedimenti formali (a livello parlamentare, come in Italia), lettere aperte o altro, su molti temi connessi all'e-government i garanti europei hanno potuto far sentire la propria voce.
- Un altro punto fermo è l'esistenza di un grande numero di progetti in via di realizzazione in tutti i Paesi UE, molti dei quali hanno implicazioni significative sui trattamenti di dati personali dei cittadini: citiamo, in particolare, la possibilità di presentare dichiarazioni dei redditi online e di effettuare pagamenti specifici (IVA), notificare cambiamenti di residenza, consultare offerte di lavoro, e tutta una serie di servizi (prestiti bibliotecari, rilascio di permessi edilizi o certificati anagrafici, esami universitari, rimborsi di spese sanitarie, ecc.). In questi casi le autorità consultate hanno sottolineato, naturalmente, l'esigenza di specifiche misure di sicurezza (identificazione e autenticazione, cifratura dei dati trasmessi) e di un'adeguata informazione dei cittadini – in particolare, rispetto ai diritti riconosciuti dalla direttiva e dalle leggi nazionali (accesso, rettifica, cancellazione).
- Nella maggioranza dei Paesi UE sono già disponibili (o lo saranno presto) veri e propri portali della pubblica amministrazione, ossia punti di accesso unici dai quali è possibile raggiungere più amministrazioni (centrali o periferiche) e, in alcuni casi, ottenere vari servizi (secondo il modello dello "sportello unico"). Ciò comporta l'esigenza di raccogliere e conservare dati personali, e nei Paesi ove queste iniziative sono in fase più avanzata (ad esempio, nei Paesi Bassi) l'autorità per la privacy ha richiamato l'attenzione sull'esigenza di specificare chiaramente compiti e responsabilità delle singole

amministrazioni che accedono al portale, e di garantire idonee misure di sicurezza. Un'altra questione rilevante riguarda la possibilità di servirsi di soggetti privati per la gestione di alcune di queste procedure amministrative. Sul tema le opinioni divergono: alcuni Paesi, fra cui l'Italia, non ritengono possibile che soggetti privati accedano ai dati personali dei cittadini che si rivolgono alla pubblica amministrazione (anche se in molti di tali Paesi i portali sono stati sviluppati con tecnologie messe a disposizione da soggetti privati); in altri (ad esempio in Francia o in Belgio) ciò è invece ritenuto possibile, ma i soggetti privati devono dare idonee garanzie di affidabilità soprattutto in termini di tutela della privacy dei cittadini. Ad ogni modo, i requisiti individuati da varie autorità per consentire il coinvolgimento di soggetti privati nella gestione dei portali della pubblica amministrazione comprendono la previsione di adeguate garanzie contrattuali; l'indicazione precisa dei compiti affidati; la definizione di misure di sicurezza; il divieto di utilizzare i dati per finalità diverse da quelle per cui sono stati raccolti e di comunicarli a terzi; la specificazione dei dati conservati, e l'eventuale previsione di una commissione indipendente di controllo.

- Il problema del codice di identificazione unico. In molti paesi esiste già un "identificatore" unico utilizzato dai cittadini per i contatti con la pubblica amministrazione. Può trattarsi di un identificatore settoriale (codice fiscale italiano) oppure di un numero unico nazionale (Svezia, Finlandia). La riflessione dei Garanti si è concentrata su due temi fondamentali: a) il fatto che l'impiego su scala generale di identificatori originariamente settoriali necessita di adeguate garanzie (in pratica, di un fondamento di legge così come richiesto dalla direttiva 95/46). E' il caso dell'Italia e del previsto ampliamento delle possibilità di utilizzazione del codice fiscale (va ricordato, inoltre, che, ad esempio, in Portogallo esiste un divieto costituzionale di introdurre un identificatore unico nazionale); b) i rischi di un'interconnessione "selvaggia" fra database diversi attraverso, appunto, l'identificatore unico. Anche in questo caso devono esistere idonee garanzie legislative che vietino ai soggetti pubblici di utilizzare per finalità diverse i dati raccolti e conservati, tranne nei casi previsti specificamente dalla legge.
- Per quanto riguarda, più in generale, i rischi connessi all'interconnessione fra banche dati della pubblica amministrazione, tutte le Autorità si oppongono a forme indiscriminate di interconnessione. Tutte hanno sottolineato che le opportunità di semplificazione e razionalizzazione offerte dallo sviluppo dell'e-government non devono tradursi in un aumento dei controlli sui cittadini. In molti Paesi sono stati istituiti specifici gruppi di lavoro, ai quali partecipano le autorità di protezione dati per valutare esattamente questi aspetti. Ancora una volta, i principi che devono essere fatti valere ai fini dell'interconnessione (regolamentata per legge) sono quelli della qualità dei dati (i dati personali devono essere adeguati, pertinenti, non eccedenti), della legittimità dei trattamenti, dell'informazione agli interessati e di un elevato livello di sicurezza. Particolare interesse rivestono i risultati di uno studio condotto dal Governo del Regno Unito, che ha evidenziato come i benefici attesi dalla condivisione delle informazioni pubbliche non debbano essere considerati prevalenti sulle attese dei cittadini rispetto alla tutela della loro privacy.
- Piuttosto limitata risulta nei 15 Paesi europei l'esperienza legata all'attuazione della firma digitale. Sono pochi i settori nei quali è possibile servirsi della firma digitale, per motivi di vario genere (costi elevati, assenza di norme regolamentari, complessità dei sistemi esistenti). Ad ogni modo, tutti i Garanti hanno giudicato positivamente la firma digitale in quanto possibile ausilio per offrire una migliore tutela dell'identità personale; hanno però sottolineato che è fondamentale prevedere un'adeguata e chiara informazione degli utenti da parte dei servizi di certificazione (destinatari delle informazioni raccolte, misure di sicurezza etc.).
- Carta di identità elettronica: nella maggior parte dei Paesi UE esistono carte elettroniche di identità di natura settoriale, utilizzate per servizi specifici (generalmente di tipo sanitario). In tutti questi Paesi è previsto un ampliamento dell'uso di tali carte, anche se non sempre esse serviranno ai fini dell'identificazione dei cittadini su base generalizzata. Le autorità nazionali sono state consultate in varia misura (come sopra ricordato) rispetto a tali progetti, ed hanno segnalato alcuni aspetti problematici: definizione delle categorie di dati registrabili sulla carta, procedure da utilizzare per il trattamento di tali dati, definizione dei soggetti autorizzati ad accedere alle diverse categorie di dati, rispetto dei diritti delle persone, possibilità di utilizzare la carta elettronica per finalità commerciali (pagamenti on line, "portafogli elettronico"). E' interessante osservare che l'Italia risulta essere, insieme alla Finlandia, il Paese nel quale la sperimentazione di questo tipo di carta di identità è maggiormente avanzata.

Indirizzi di posta elettronica non sono assimilabili a quelli su elenchi pubblici: comunicazione del Garante per la protezione dei dati personali

NUMERO SCHEDA: 2381

CLASSIFICAZIONE: ATTIVITA' E ATTI AMMINISTRATIVI

SOTTOCLASSIFICAZIONE: Privacy

FONTE: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DATA: 16/02/2003

NATURA ATTO: COMUNICAZIONE

DATA ATTO: 16/02/2003

ORGANO: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella newsletter del 16.02.2003, il Garante per la protezione dei dati personali ribadisce la non assimilabilità degli indirizzi e-mail presenti in rete ad indirizzi presenti su elenchi pubblici.
Secondo il Garante la vasta conoscibilità degli indirizzi e-mail che Internet consente non rende lecito l'uso di questi dati personali per scopi diversi da quelli per i quali sono presenti on line, di conseguenza gli indirizzi e-mail non possono essere considerati "pubblici" come possono essere quelli presenti sugli elenchi telefonici .
Il Garante afferma che "La circostanza che l'indirizzo e-mail sia conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti non lo rende, infatti, liberamente utilizzabile e non autorizza comunque l'invio di informazioni, di qualunque genere, anche se non specificamente a carattere commerciale o promozionale, senza un preventivo consenso".

Si allega il testo della newsletter.

Garante per la protezione dei dati personali,
Newsletter 10 - 16 febbraio 2003
PRIVACY SU INTERNET. GLI INDIRIZZI E-MAIL NON SONO PUBBLICI
Gli indirizzi di posta elettronica non sono liberamente utilizzabili da chiunque per il solo fatto di trovarsi in rete. La vasta conoscibilità degli indirizzi e-mail che Internet consente, non rende lecito l'uso di questi dati personali per scopi diversi da quelli per i quali sono presenti on line. Gli indirizzi e-mail non sono, insomma, "pubblici" come possono essere quelli presenti sugli elenchi telefonici.
Il principio è stato ribadito dall'Autorità Garante (composta da Stefano Rodotà. Giuseppe Santaniello, Gaetano Rasi e Mauro Paissan) che ha affrontato in questi ultimi mesi diversi casi di utenti che avevano segnalato la pratica ormai diffusa di inviare e-mail commerciali ad indirizzi di posta elettronica raccolti in rete. Alle proteste degli utenti, le società che avevano inviato le e-mail rispondevano che non vi era stata alcuna violazione della privacy perché gli indirizzi erano stati reperiti su Internet (spesso attraverso appositi software) e che pertanto erano "pubblici".
Niente di più sbagliato, afferma l'Autorità. Gli indirizzi di posta elettronica non provengono, infatti, da pubblici registri, elenchi, atti o documenti formati o tenuti da uno o più soggetti pubblici e non sono sottoposti ad un regime giuridico di piena conoscibilità da parte di chiunque. La circostanza che l'indirizzo e-mail sia conoscibile di fatto, anche momentaneamente, da una pluralità di soggetti non lo rende, infatti, liberamente utilizzabile e non autorizza comunque l'invio di informazioni, di qualunque genere, anche se non specificamente a carattere commerciale o promozionale, senza un preventivo consenso.

L'Autorità sottolinea che l'eventuale disponibilità in Internet di indirizzi di posta elettronica, anche se resi conoscibili dagli interessati per certi scopi (ad esempio su un sito istituzionale o anche aziendale) attraverso siti web o newsgroup, va "rapportata alle finalità per cui essi sono pubblicati sulla rete". A maggior ragione questo principio vale in caso di uso indebito di software che rastrellano automaticamente migliaia di indirizzi in rete o li creano "a tavolino" a prescindere da un accertamento sulla loro effettiva esistenza.
Per poter inviare e-mail senza violare la privacy degli utenti web è obbligatorio, dunque, ottenere prima il loro consenso.
Uno degli ultimi casi di cui si è occupato il collegio del Garante ha riguardato un docente che si era visto recapitare una e-mail pubblicitaria al proprio indirizzo di posta elettronica, presente per finalità di istituto, sul sito dell'università presso la quale insegna.

La pubblicità dell'indirizzo di posta elettronica non legittima di per sè l'invio di messaggi pubblicitari.

NUMERO SCHEDA: 1599

CLASSIFICAZIONE: ATTIVITA' E ATTI AMMINISTRATIVI

SOTTOCLASSIFICAZIONE: Privacy

FONTE: IL SOLE 24 ORE

NUMERO: 182

DATA: 06/07/2002

PAGINA: 18

NATURA ATTO: MESSAGGIO

DATA ATTO: 30/06/2002

ORGANO: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il Garante ha precistato che l'indirizzo di posta elettronica contenuto in un sito, pur essendo pubblico, non legittima le aziende ad inviare messaggi pubblicitari in quanto deve tenersi conto della ragione per cui l'indirizzo è pubblicato.
Di conseguenza l'utilizzo del medesimo è consentito esclusivamente per finalità determinate e quindi il titolare dell'indirizzo può ottenere la cancellazione del suo nomitativo negli archivi di terzi al fine di evitare un utilizzo indiscrimitato e dannoso del dato.

Si riporta qui di seguito la newsletter.

La presenza dell' indirizzo e-mail di una persona su un sito Internet non autorizza le aziende, per il solo fatto di essere pubblico, ad utilizzarlo per inviare pubblicità.
Lo ha stabilito il Garante affrontando il caso di un docente che si era visto recapitare una e-mail pubblicitaria al proprio indirizzo di posta elettronica, presente, per finalità istituzionali, sul sito dell'università presso la quale insegna. L'interessato aveva fatto presente alla società la propria contrarietà all'uso dei dati personali che lo rigurardano per scopi di informazione commerciale. Non soddisfatto delle risposte ricevute, si era rivolto al Garante per ribadire la sua opposizione all'utilizzo

dei propri dati personali e perché la società si comportasse di conseguenza, chiedendo inoltre di porre a carico della stessa le spese del procedimento.
Nel corso dell'istruttoria è risultato che la società, nel rispondere alla richiesta dell'interessato, aveva comunicato di detenere sì nel proprio data base i dati personali del personale, ma di averli inseriti in una lista di soggetti non disponibili a ricevere materiale pubblicitario. La società aveva comunicato, inoltre, di aver desunto l'indirizzo e-mail del docente dal sito Internet dell'Università.
Il Garante ha ribadito che la pubblicità di alcuni indirizzi, resi conoscibili attraverso i siti Internet, va collegata agli scopi per i quali questi indirizzi vengono resi noti. I dati posti a disposizione del pubblico per circoscritte finalità, ad esempio di tipo istituzionale come nel caso in esame, non sono, infatti, liberamente utilizzabili per l'invio generalizzato di e-mail. E questo anche quando le e-mail non abbiano un contenuto commerciale o pubblicitario.
Per poter procedere all'invio dell'e-mail all'indirizzo di posta elettronica del docente, la società avrebbe dovuto, dunque, ottenere prima il suo consenso. Non vendo né richiesto né ottenuto tale consenso la società ha, pertanto, violato le norme sulla privacy. Di conseguenza, la società non poteva limitarsi ad inserire il nominativo del ricorrente in una lista di soggetti non interessati all'invio di messaggi pubblicitari, ma aveva l'obbligo di cancellare i dati del ricorrente ed astenersi in futuro dall'utilizzare quei dati per scopi commerciali l'indirizzo e-mail presso l'università.
L'Autorità ha, dunque, ordinato alla società di conformarsi a queste indicazioni e ha posto a carico della società, così come richiesto dal ricorrente, le spese del procedimento, determinate nella misura forfetaria di 250 euro.

Il Garante per la protezione dei dati personali "condanna" una società che inviava e-mail pubblicitarie senza consenso

NUMERO SCHEDA: 1446

CLASSIFICAZIONE: ATTIVITA' E ATTI AMMINISTRATIVI

SOTTOCLASSIFICAZIONE: Privacy

FONTE: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NUMERO: 128

DATA: 19/05/2002

RIFERIMENTO NORMATIVO: legge 675/96; d.lgs. 185/99

NATURA ATTO: COMUNICAZIONE

DATA ATTO: 19/05/2002

NUM. ATTO: 128

ORGANO: GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Accogliendo in parte il ricorso di un consumatore, l'Autorità Garante ha ribadito che è illegittimo utilizzare a scopi commerciali un indirizzo e-mail, che non compare in elenchi pubblici, senza il consenso del destinatario. L'Autorità ha ordinato alla società che inviava messaggi pubblicitari non richiesti tramite posta elettronica di astenersi da ogni loro ulteriore trattamento, in particolare dell'indirizzo e-mail ed ha anche imposto alla società di rifondere al consumatore le spese sostenute per il procedimento.

Il Garante ha chiarito che, in base alla normativa vigente in materia di privacy e di protezione dei consumatori (legge 675/96 e d.lgs. 185/99), nei contratti a distanza l'invio di materiale pubblicitario rientra nei casi in cui è vietato l'impiego della posta elettronica da parte di un fornitore senza il consenso preventivo del consumatore.
Il Garante ha inoltre ritenuto di dover procedere d'ufficio all'apertura di un procedimento autonomo per la verifica della liceità e della correttezza del trattamento complessivo dei dati e per valutare i presupposti per l'applicazione di eventuali sanzioni. Ha dichiarato, invece, inammissibile la richiesta di risarcimento dei danni che può essere rivolta solo al giudice ordinario.
La società, che non aveva dato immediato riscontro all'istanza dell'interessato, è stata "condannata" al pagamento di 250 euro per le spese del procedimento, da versare al consumatore

Rapporti tra privacy ed e-mail

NUMERO SCHEDA: 988

CLASSIFICAZIONE: ATTIVITA' E ATTI AMMINISTRATIVI

SOTTOCLASSIFICAZIONE: Privacy

FONTE: ITALIA OGGI

DATA: 13/11/2001

NATURA ATTO: MESSAGGIO

DATA ATTO: 11/11/2001

Il Garante della privacy, con un recente provvedimento, ha affermato che il lavoratore può accedere alle e-mail che contengono i suoi dati personali. L'azienda deve infatti consentire al dipendente che ne faccia richiesta l'accesso a tutte le informazioni personali e alle valutazioni professionali che lo riguardano, anche se contenute nella posta elettronica dell'azienda. E per quanto non sia obbligata ad esibire o copiare ogni documento, l'azienda deve comunque estrarre dagli atti tutte le informazioni relative al solo interessato e comunicargliele in modo facilmente comprensibile. Il Garante ha ribadito che l'ampia definizione di dato personale adottato dalla direttiva comunitaria e dalla legge sulla privacy comprende non solo dati di tipo oggettivo (nome,cognome, data di nascita, ecc.), ma anche altri dati personali contenuti in valutazioni soggettive, ispezioni, relazioni. E' quindi legittima la richiesta di accesso del dipendente per conoscere il contenuto delle e-mail che contengono tali valutazioni.

Si allega il testo della newsletter del Garante della privacy.

Lavoratori e dati personali contenuti nelle e mail aziendali

L'azienda deve consentire al dipendente che ne faccia richiesta, l'accesso a tutte le informazioni personali e le valutazioni professionali che lo riguardano, anche a quelle contenute nella posta elettronica dell'azienda. E per quanto non sia obbligata ad esibire o copiare ogni documento, l'azienda deve comunque estrarre dagli atti tutte le informazioni relative al solo interessato e comunicargliele in modo facilmente comprensibile.

I principi sono stati sanciti dal Garante, che ha accolto il ricorso di un funzionario di una società, che aveva richiesto di conoscere il contenuto di alcune e-mail indirizzate, da altri dipendenti, al dirigente del dipartimento risorse umane, e nelle quali si esprimevano giudizi professionali che erano poi stati alla base di un procedimento disciplinare nei suoi confronti. La società, su invito del Garante ad aderire alle richieste del ricorrente, ha fatto pervenire al dipendente le copie di tre messaggi, in cui erano stati cancellati i riferimenti ai mittenti e alle altre persone citate. La comunicazione è stata giudicata incompleta ed inesatta dall'interessato, che ha ribadito le istanze presentate nel ricorso.
Nel provvedimento, il Garante ha ribadito che l'ampia definizione di dato personale adottata dalla direttiva comunitaria e dalla legge sulla privacy comprende non solo dati di tipo oggettivo (nome, cognome, data di nascita etc.), ma anche altri dati personali contenuti in valutazioni soggettive, ispezioni, relazioni etc., in possesso dell'azienda. E' quindi legittima la richiesta di accesso del dipendente per conoscere il contenuto delle e-mail che contengono tali valutazioni. In questo caso, ha poi precisato l'Autorità, non si è di fronte a trattamenti effettuati da persone fisiche per fini personali, per i quali non si applica la legge sulla privacy: i dati richiesti dall'interessato sono, infatti, contenuti in comunicazioni inoltrate al responsabile del personale, da altri dipendenti, per finalità di tipo professionale, legate all'attività dell'azienda.
Per quanto riguarda, inoltre, la comunicazione dei dati, il Garante precisa che la normativa vigente non prevede come necessario il rilascio di copie di atti, ma obbliga il titolare o il responsabile del trattamento ad estrapolare dai propri archivi, cartacei o informatizzati, i dati personali conservati e a riferirli al richiedente in modo comprensibile. L'accesso, in questo caso non obbliga quindi a fornire copia delle e-mail, che nell'intestazione possono rivelare altri dati relativi al mittente, ma a comunicare le informazioni del richiedente in esse contenute. Solo se l'estrapolazione risulti particolarmente difficoltosa si può esibire o consegnare copia della documentazione, priva però dei dati riferiti ad altri soggetti.

Appendice

APPENDICE

Siti

In questa sezione sono raccolti alcuni siti di particolare rilievo nell'ambito delle materie dell'e-government e dell'informatica.

L'indirizzo di ogni sito è seguito da una breve spiegazione sul contenuto e sull'articolazione dello stesso.

I portali recensiti sono raggruppati in tre sottosezioni: "Siti istituzionali", "Siti privati" e "Siti del Piemonte".

All'interno di ciascuna sottosezione i siti sono riportati seguendo l'ordine alfabetico.

SITI ISTITUZIONALI

http://www.cnipa.gov.it/site/it-IT/

Sito del CNIPA, il Centro Nazionale per l'Informatica nella Pubblica Amministrazione, che opera presso la Presidenza del Consiglio per l'attuazione delle politiche del Ministro per l'Innovazione e le Tecnologie.
Unifica in sé due organismi preesistenti: l'Autorità per l'informatica nella pubblica amministrazione ed il centro tecnico per la R.U.P.A.
Il CNIPA ha l'obiettivo primario di dare supporto alla pubblica amministrazione nell'utilizzo efficace dell'informatica per migliorare la qualità dei servizi e contenere i costi dell'azione amministrativa.
In sintesi il CNIPA:
contribuisce alla definizione della politica del Governo e del Ministro per l'innovazione e le tecnologie e fornisce consulenza per la valutazione di progetti di legge nel settore informatico;

- coordina il processo di pianificazione e i principali interventi di sviluppo; detta norme e criteri per la progettazione, realizzazione, gestione dei sistemi informatici delle amministrazioni, della loro qualità e dei relativi aspetti organizzativi; definisce criteri e regole tecniche di sicurezza, interoperabilità, prestazione;
- controlla che gli obiettivi e i risultati dei progetti di innovazione della pubblica amministrazione siano coerenti con la strategia del Governo; a tale scopo si affianca alle amministrazioni pubbliche nella fase di progettazione ed emette pareri di congruità tecnico-economica;
- cura l'attuazione di importanti progetti per l'innovazione tecnologica nella pubblica amministrazione, la diffusione dell'e-government e lo sviluppo delle grandi infrastrutture di rete del Paese per consentire agli uffici pubblici di comunicare tra loro e per portare i servizi della pubblica amministrazione ai cittadini e alle imprese;

- cura la formazione dei dipendenti pubblici nel settore informatico, utilizzando le nuove tecnologie per favorire l'apprendimento continuo.

Dal punto di vista organizzativo il CNIPA è governato da un organo collegiale costituito dal Presidente e da quattro membri, scelti tra persone dotate di alta e riconosciuta competenza e professionalità, nominati dal Presidente del Consiglio dei Ministri.
La homepage presenta, in posizione centrale, tutte le principali novità, mentre sulla sinistra e sulla destra dello schermo vi sono diverse sezioni tematiche, suddivise in una pluralità di sottosezioni.
Sulla sinistra: la presentazione de "Il Centro Nazionale", le "Areee Operative", "In primo piano", "Attività", "Bandi e Avvisi". Sulla destra: la sezione dedicata alla "Sala stampa". Seguono "Normativa", "Documentazione", "Eventi CNIPA", "Link" e "Archivio Link".

http://www.crcitalia.it

Portale dei Centri Regionali di Competenza per l'e-government e la società dell'informazione, che sono una rete di strutture territoriali che, grazie ad un accordo tra il Ministro per l'Innovazione e le Tecnologie e le singole Regioni, supportano le amministrazioni locali nella diffusione delle nuove tecnologie nel loro territorio.
Il progetto CRC, nato nella primavera 2002, è attuato dal Formez, e ha le finalità di:

- sviluppare la cooperazione tra le strutture di cui si avvale il MIT e i sistemi regionali, mettendo in rete i CRC in un network nazionale, rappresentativo del nuovo assetto istituzionale federalista;
- supportare le attività della Commissione Permanente per l'Innovazione e le Tecnologie;
- supportare gli Enti Locali e rafforzarne le competenze nella definizione ed attuazione di programmi e progetti per l'e-government e la società dell'informazione, in coerenza con gli obiettivi fissati dalle Linee Guida del governo e della Visione Condivisa;
- definire e diffondere modelli, approcci e strumenti condivisi e integrati sugli aspetti critici della realizzazione dei processi di innovazione;
- sviluppare la cooperazione ed il coordinamento tra diversi livelli di governo nei sistemi regionali e favorire scambi e azioni comuni su scala interregionale.

La rete è organizzata in uno Staff Centrale, attivato presso il Formez, che garantisce l'attuazione del progetto, e in 20 Centri (CRC) attualmente attivati presso le singole Regioni, costituiti sulla base di apposite Convenzioni tra il Ministro per l'innovazione e le tecnologie (MIT) e i Presidenti delle Regioni e delle Province Autonome.
I CRC sono strutture snelle e fortemente operative, attivate da gruppi locali (detti Team di progetto) di funzionari e dirigenti di diversi livelli di governo, affiancati da personale messo a disposizione sia dal Formez su incarico del MIT, sia eventualmente da società convenzionate su incarico delle Regioni. I CRC svolgono un ruolo di raccordo rispetto al sistema delle PA locali del territorio, fornendo loro servizi informativi, formativi e di assistenza progettuale.
Centralmente sono riportate le "News", sulla sinistra della homepage c'è l'agenda degli incontri e seminari, mentre sulla sinistra vi sono moltissime rubriche, fra le quali si segnalano: "e-Government fase I", "e-Government: fase II", "Focus", "Pubblicazioni e Servizi".

http://www.forumpa.it/canali/altrapa/index.html

Canale tematico di FORUM P.A. dedicato al tema dell'innovazione tecnologica nella pubblica amministrazione. Presenta una selezione di esperienze, documentazione, interviste e contributi di esperti per capire come le nuove tecnologie possono migliorare il modo di governare e gestire i processi amministrativi.
Si articola in tante sezioni. Grande rilievo è dato a "Reti" e "Processi". Vi sono poi i "dossier", gli "studi", la sezione delle norme (nella quale sono raccolte le principali fonti normative e regolamentari in materia di informatizzazione della pubblica amministrazione ed i documenti di indirizzo sull'e-government, suddivise per aree tematiche) e quella che raccogli gli articoli, quella degli "appuntamenti", quella delle "news" e molte altre ancora.

http://www.innovazione.gov.it/

Sito del Ministro per l'Innovazione e le Tecnologie, articolato in diverse sezioni e sottosezioni.
Il Ministro per l'Innovazione e le Tecnologie ha, per delega del Presidente del Consiglio dei Ministri, la responsabilità di coordinare ed indirizzare la politica del Governo in materia di sviluppo e di impiego delle Tecnologie dell'Informazione e delle Comunicazioni (ICT) nel Paese, in particolare nell'economia, nelle Pubbliche Amministrazioni, centrali e locali, nelle famiglie, allo scopo di promuovere lo sviluppo della "Società dell'Informazione" nel nostro Paese ed a tal fine presiede il Comitato dei Ministri per la Società dell'Informazione.
La parte centrale della homepage è dedicata alle sezioni delle "Novità", delle "Iniziative" , alla sezione "In Evidenza" e ai "Link".
Sulla destra i "Comunicati Stampa", "Newsletter", "Pubblicazioni", "Extra".
Sulla sinistra "Ministro on line", "Dipartimento", "Sala stampa", "Linee di azione del Ministro", "Atti normativi e documenti", "E-government per lo sviluppo", "E-government", "Società dell'informazione" e "Link utili".

http://www.iit.cnr.it/

Il 1 marzo 2002 è divenuto operativo il nuovo Istituto di Informatica e Telematica (IIT) del CNR, nato dalla fusione dell'Istituto per le Applicazioni Telematiche con l'Istituto di Matematica Computazionale.
L'Istituto svolge attività di ricerca, valorizzazione e trasferimento tecnologico e di formazione nel settore delle tecnologie dell'informazione e della comunicazione e nel settore delle scienze computazionali.
Lo IIT svolge la funzione di Registro del ccTLD ".it", responsabile dell'assegnazione dei nomi a dominio all'interno del country code top level domain ".it" (ISO 3166). Questo ruolo è stato riconosciuto da IANA (Internet Assigned Numbers Authority) fino dal 1987 e successivamente da ICANN (The Internet Corporation for Assigned Names and Numbers). Lo IIT interagisce con oltre 2000 provider/maintainer. I nomi a dominio registrati attualmente nel ccTLD "it" sono oltre 700 mila.

http://www.padigitale.it/home/home.html

E' questo un sito interamente dedicato al Codice dell'amministrazione digitale.
Il documento più importante in materia di e-government ha così un sito ad esso interamente dedicato ed articolato in più sezioni.
La sezione più importante "Il Codice della PA digitale", si articola nelle seguenti parti:

- Presentazione
- Cosa è
- I nuovi diritti
- Gli strumenti
- Le novità
- I vantaggi
- Il testo del decreto

"Il Codice spiegato da" contiene diversi video con i quali esperti in materia di innovazione tecnologica parlano del Codice.
Nella sezione "Per approfondire" si possono trovare i principali documenti in materia e i link.
Si segnala infine la possibilità di inviare un commento sul codice o di porre quesiti ad esperti sul medesimo.

http://www.protocollo.gov.it/

Sito a cura del Centro di Competenza per il Progetto Protocollo informatico e trasparenza amministrativa, istituito presso il Cnipa mediante la Direttiva MIT del 9/12/2002 sulla trasparenza dell'azione amministrativa e gestione elettronica dei flussi documentali, che svolge funzioni di indirizzo e di coordinamento ed offre alle amministrazioni assistenza e consulenza per valutare i propri programmi di sviluppo nel settore.
A partire dal 1° gennaio 2004, il Cnipa è titolare di compiti, funzioni ed attività esercitate in precedenza dall'AIPA e dal Centro Tecnico per la R.U.P.A.
Da un punto di vista organizzativo, il Centro di Competenza fa parte dell'Ufficio di Efficienza organizzativa nella P.A.C. ed opera nell'Area "Progetti, applicazioni e servizi".
Sulla sinistra ci sono le sezioni delle "Informazioni generali", "Progetti P.A.", "Supporto" e un'area riservata.
Centralmente campeggiano le News, mentre sulla sinistra si segnala la sezione "In evidenza".

http://www.pubbliaccesso.gov.it/

Progetto nato dalla collaborazione tra il CNIPA e la Commissione interministeriale permanente per l'impiego delle ICT a favore delle categorie deboli o svantaggiate, il portale offre informazioni e documentazione utile sull'accessibilità dei siti web e dei servizi in rete.

Nelle quattro sezioni sulla sinistra della homepage ("Notizie", "Eventi", "Biblioteca", "Normative"), si possono trovare informazioni sulla normativa, la documentazione, la manualistica, i quaderni e gli eventi relativi al tema dell'accessibilità e dell'inclusione informatica.
Centralmente sono riportate le novità, mentre sulla destra la sezione "In primo piano" contiene la normativa e in documenti più recenti.

SITI PIEMONTE

http://www.csi.it/home.shtml

Dal 1977 il CSI-Piemonte promuove l'innovazione della Pubblica Amministrazione locale attraverso l'impiego dei più moderni strumenti informatici e telematici.
Grazie al suo contributo, il Piemonte si presenta sulla scena italiana e internazionale come un sistema amministrativo integrato e dotato delle necessarie infrastrutture tecnologiche.
In primo piano la rubrica "Notizie" e il piano di attività 2005.
In alto varie sezioni: "consorzio", "progetti e servizi", "novità", "gare", lavora con noi", "conrtatti".

http://www.ruparpiemonte.it/

RuparPiemonte è la Rete Unitaria della Pubblica Amministrazione Regionale a cui possono aderire tutti gli Enti locali piemontesi. Realizzata, promossa e finanziata dalla Regione Piemonte, RuparPiemonte mette in comunicazione le amministrazioni, semplificando lo scambio di informazioni e di esperienze e favorendo economie di scala. Centro tecnico di gestione della rete è il CSI.
Nella homepage RuparPiemonte è illustrato nelle tre sezioni "RuparPiemonte conviene", "RuparPiemonte connette£ e "RuparPiemonte cresce". Sulla destra la rubrica "In primo piano", con gli aggiornamenti.
Fra le varie sezioni si segnala quella dedicata all'e-government e quella relativa al catalogo dei servizi.

http://www.sistemapiemonte.it/index.shtml

SistemaPiemonte è un progetto avviato nel 2000 dal CSI-Piemonte per offrire ai cittadini e alle imprese un punto di accesso unico, semplice e organizzato per ricercare i servizi e le informazioni della Pubblica Amministrazione piemontese. Grazie alla fattiva collaborazione tra la Regione Piemonte, la Provincia e la Città di Torino e tutti gli Enti locali del territorio, l'insieme degli Enti pubblici piemontesi si presenta sul portale Internet come un sistema regionale integrato, coeso e avanzato, capace di

- rinnovarsi e modernizzarsi in linea con i principi di e-government

- trasmettere dei modelli di lavoro
- progettare servizi all'avanguardia ed efficienti
- utilizzare anche tecnologie e strumenti innovativi per comunicare con i propri utenti
- migliorare i rapporti tra le amministrazioni, i cittadini, le imprese e le diverse componenti sociali
- garantire maggiore trasparenza alle azioni

Il portale offre a cittadini e imprese la possibilità di registrarsi e accedere ai servizi, di essere riconosciuti dagli Enti di competenza, di effettuare pagamenti e trasmettere dati via Internet in modo sicuro e nel rispetto delle regole sulla privacy.
La parte centrale della homepage è dedicata alle novità, mentre sulla destra è segnalato il percorso per la registrazione e vi sono diverse sezioni.

SITI PRIVATI

www.interlex.it

InterLex è un periodico plurisettimanale di carattere informativo, scientifico, culturale e giuridico, diviso in numerose sezioni tematiche cui si accede dalla prima pagina.
Nella sezione "attualità" sono presenti due indici : il primo raccoglie gli articoli, i commenti e gli studi che vanno dal 2001 al 2005; il secondo elenca quelli dal 1997 al 2000. Tutti gli articoli, al loro interno contengono link alle fonti citate, siano esse giurisprudenziali, dottrinali o normative.Vi sono di seguito sezioni tematiche (Dati personali (L. 675/96);Firma digitale;E - commerce;Le regole dell'internet;Nomi a dominio;Diritto d'autore Internet e stampa;Diritto di accesso;Pubblica amministrazione;Telecomunicazioni;Europa).
Tra queste si segnala la sezione "dati personali (L. 675/96)" che raccoglie i documenti dal 1995 al 2002 tra cui le newsletter del garante, i comunicati stampa e gli altri provvedimenti del garante.La sezione "firma digitale" è particolarmente utile perché oltre a contenere la normativa e le domande pervenute al sito - corredate dalle relative risposte - reca anche un elenco dei certificatori accreditati.
Nella sezione "le regole dell'internet" vi sono delle sottovoci tra cui segnaliamo "nomi a dominio" contenente una raccolta delle sentenze dei tribunali italiani, aggiornate al 2005 (le pronunce più recenti sono comunque inserite nell'apposita sezione "nomi a dominio"); una sottovoce interamente dedicata al d.lgs. 103/95 e le autorizzazioni generali; la sottovoce "riforma delle telecomunicazioni" che contiene gli approfondimenti sul diritto di acceso agli atti amministrativi anche in relazione all'informatizzazione della p.a. Infine la sezione dedicata interamente alla p.a. è ulteriormente suddivisa in due sottovoci: la prima contiene le norme sul protocollo informatico e la gestione documentale, la seconda quelle sul documento informatico.
Il sito inoltre segnala convegni e seminari che interessino il processo di informatizzazione della p.a. e l'innovazione tecnologica in generale e recensisce i libri pubblicati sui medesimi temi.
Inoltre il sito dispone di un motore di ricerca ed è dotato di un indice sistematico applicato a tutte le sezioni su menzionate, un indice generale dei documenti (dal 1997)

nonchè una sezione dedicata ai numeri precedenti della rivista (fino al 1997), ordinati cronologicamente.

www.scint.it

Il sito scint.it è curato e coordinato dallo Studio Associato D.&L., di Lecce, ed è ospitato sui server del servizio Aruba.it. Il sito è espressione di un Centro Studi (Associazione senza fini di lucro denominata "SCINT") e viene aggiornato senza alcuna periodicità, esclusivamente sulla base della disponibilità del materiale.
Dispone di numerose sezioni tematiche (Unione Europea Innovazione tecnologica Commercio Internazionale, Sviluppo e territorio, Unione Europea) contenenti articoli e saggi.
Si segnala inoltre la sezione "formazione" che reca il programma dei corsi organizzati dal centro Studi e ricerche SCINT e informazioni utili per trovare stages presso studi professionali, aziende ed enti pubblici.
Un'altra sezione particolarmente interessante è quella intitolata "utilità" che contiene documenti tratti da altri siti, un link alla Home page dell'Ufficio Italiano cambi e, fra gli altri, un link al sito http://www.emarketservices.it/ che nasce dalla collaborazione tra l' ICE (Istituto nazionale per il Commercio Estero) e le principali Agenzie per la promozione del commercio estero europee con lo scopo di pro-muovere l'e-Business presso le piccole e medie imprese dei paesi membri a supporto dei processi di internazionalizzazione. Per completezza pare opportuno precisare che l'elenco completo dei collegamenti agli altri siti è contenuto nella sezione apposita "links".
Inoltre, per facilitare il reperimento veloce delle informazioni è disponibile un motore di ricerca, un servizio gratuito di newsletter. Invece per gli eventuali approfondimenti è disponibile una sezione dedicata alla segnalazione di convegni, seminari ed altri eventi formativi.

www.nir.it

1)Il progetto

E' il portale di accesso alle norme pubblicate sui siti delle P.A. partecipanti.Sul sito si può leggere la storia del progetto che ha portato alla sua istituzione. In particolare si legge che nel gennaio 1999 si avvia il progetto intersettoriale NormeinRete, proposto dal Ministero della Giustizia, coordinato e finanziato dall'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA).Nel gennaio 2000 L'Istituto per la Documentazione Giuridica (IDG, ora ITTIG) del Consiglio Nazionale delle Ricerche consegna lo studio di fattibilità per la realizzazione del sistema. Nel febbraio-marzo 2000 si costituiscono quattro "Gruppi di lavoro" interistituzionali, cui è affidato lo studio delle problematiche relative alla standardizzazione assumendo come riferimento linguaggi e tecniche emergenti nel mondo Internet .Il medesimo anno il CINECA (Consorzio Interuniversitario del Nord Est Italiano per il Calcolo Automatico) realizza la prima versione del portale NormeinRete.
Nel mese di maggio del 2000 si conclude la fase sperimentale del progetto NiR: le amministrazioni partecipanti sono 18, la base documentale è costituita da oltre 40.000 documenti e il sito registra una media di 25.000 ricerche al mese

Nel settembre 2000 si costituisce un Comitato tecnico interistituzionale, presieduto dall'AIPA, con compiti di indirizzo e di supervisione: ne fanno parte il Senato della Repubblica, la Camera dei deputati, la Presidenza del Consiglio, il Ministero della giustizia, la Corte di cassazione.Nel 2001 si pubblica sul sito Normeinrete la prima versione del Catalogo delle norme, realizzato con l'intento di censire e classificare l'intero corpus normativo italiano indipendentemente dalla disponibilità dei documenti in rete. Nel medesimo anno l'Autorità per l'informatica nella PA emana la circolare AIPA/CR/35 sulle "Regole per l'assegnazione di nomi uniformi ai documenti giuridici" (GU n. 262 del 10/11/2001)
Nel novembre 2001 iniziano a Roma le sessioni di formazione sul linguaggio XML riservate alle amministrazioni partecipanti.Nell' aprile 2002 L'Autorità per l'informatica nella PA emana la circolare AIPA/CR/40 "Formato per la rappresentazione elettronica dei provvedimenti normativi tramite il linguaggio di marcatura XML" (GU n. 102 del 3 maggio 2002) .Nel maggio 2002 si conclude la prima fase del progetto NiR: il numero delle Amministrazioni partecipanti si è elevato a 40 e i documenti indicizzati sono oltre 90.000. Il sito registra una media di oltre 100.000 richieste al mese. Nel novembre 2002 la ricerca sul sito Normeinrete si dota della nuova funzione di Navigazione tra i riferimenti normativi
Infine nell'aprile 2003 è in linea la nuova versione del portale Normeinrete.

2)La descrizione del sito

L'Home page del sito si apre con un primo sistema di ricerca per norme statali e regionali. I canali di ricerca sono due: per estremi del provvedimento o per parola chiave contenuta nel provvedimento stesso. Sono accessibili dalla home page anche altri due tipi di ricerca: quella estesa e quella avanzata.La prima consente di reperire, indicando una o più parole contenute nel testo, i provvedimenti normativi pubblicati sui siti delle istituzioni che partecipano a NormeinRete. I provvedimenti che possono essere ricercati sono norme comunitarie, statali e regionali, pareri, sentenze e decisioni (pubblicate dal sito istituzionale della Corte costituzionale e dalla Corte di cassazione)nonché studi e documentazione.
La seconda viene effettuata su tutta la normativa dello Stato e delle Regioni, combinando i dati identificativi dell'atto (tipo provvedimento ed estremi) con le parole del testo e del titolo. Per ogni risultato è attivo il link al testo, reso disponibile on line dalla Corte di Cassazione.
Sono disponibili anche le banche dati specialistiche fornite da alcuni siti istituzionali come l'Agenzia delle entrate, la Corte di cassazione, il sito ANCI, il sito ARAN, il sito istituzionale di Giustizia amministrativa,la banca dati di legislazione europea, i siti di dottrina giuridica, e i codici reperibili sul sito del notariato. Sono inoltre disponibili le gazzette ufficiali pubblicate negli ultimi sessanta giorni.
Un altro servizio di particolare interesse è costituito dal collegamento con il sito istituzionale del parlamento italiano per la ricerca dei progetti di legge. In particolare tale servizio consente la ricerca di informazioni relative ai progetti di legge (PDL) presentati al Senato della Repubblica e alla Camera dei Deputati nel corso dell'attuale legislatura o in quelle precedenti, a partire dalla VIII.
Per ogni progetto di legge sono disponibili schede informative relative all'iter parlamentare (presentatori, titolo, iter legislativo, situazione attuale dell'iter, eventuali estremi della legge, termini di classificazione TE.SE.O, trattazione in Aula o

Commissione, ecc.). Ogni scheda è relativa ad una singola lettura del progetto di legge in uno dei due rami del Parlamento; una volta approvato definitivamente, un progetto di legge ha quindi almeno due schede informative, corrispondenti ai necessari passaggi alla Camera e al Senato.
Dalle schede è possibile accedere ai testi dei progetti di legge e degli eventuali altri documenti correlati (relazioni di maggioranza e di minoranza).
Inoltre il sito dispone di un servizio di newsletter gratuito e del collegamento con numerosi servizi on line offerti dalle pubbliche amministrazioni per favorire l'esercizio dei diritti e l'adempimento delle disposizioni normative da parte dei cittadini.
Infine si segnala la sezione dedicata ai link istituzionali, facilmente consultabile in quanto l'elenco è suddiviso in "siti nazionali"; "unione europea"; "siti istituzionali stranieri" e "organizzazioni internazionali".