DIGITAL AGENDA ITALIA

Il nuovo CAD

Manuale d'uso

Dipartimento per la Digitalizzazione
della Pubblica Amministrazione
e l'Innovazione Tecnologica

DIGITAL AGENDA ITALIA

Il nuovo CAD

Manuale d'uso

Edizioni FORUM PA

Questo volume è stato curato da DigitPA, dal Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica (Presidenza del Consiglio dei Ministri) e da Formez PA.

Edizioni FORUM PA
Il nuovo CAD: manuale d'uso
ISBN 9788897169048

Finito di stampare nell'aprile 2011

|SOMMARIO|

|PREMESSA|

Il 25 gennaio è entrato in vigore il nuovo CAD, il Codice dell'Amministrazione Digitale (Decreto legislativo n. 235/2010, pubblicato sulla Gazzetta Ufficiale del 10 gennaio 2011, n. 6). Dopo la riforma della pubblica amministrazione (Decreto legislativo n. 150/2009) che ha introdotto meritocrazia, premialità, trasparenza e responsabilizzazione dei dirigenti, il nuovo CAD rappresenta il secondo pilastro del processo di rinnovamento per costruire una pubblica amministrazione coerente con i criteri di efficacia, efficienza ed economicità propri dell'azione pubblica.

Il nuovo CAD completa il quadro normativo in materia di amministrazione digitale definito cinque anni or sono con il Decreto legislativo n. 82/2005, aggiornando la normativa di riferimento rispetto a un panorama tecnologico in evoluzione. Esso garantisce maggiori diritti ai cittadini e alle imprese, permettendo alle amministrazioni di lavorare meglio e di spendere più efficacemente le risorse.

Sulla base delle esperienze maturate in questi anni, il nuovo Codice introduce con chiarezza una serie di innovazioni normative volte a garantire che l'amministrazione digitale non resti solo una dichiarazione di principio, ma sia in grado di incidere effettivamente sui comportamenti e le prassi delle amministrazioni e sulla qualità dei servizi resi a cittadini e imprese.

La riforma non solo rende effettivi i diritti, accessibili le opportunità, cogenti gli obblighi, ma permette di diradare la nebbia dell'incertezza e rassicurare gli operatori sulla validità, anche giuridica, dell'amministrazione digitale.

Il Codice rende obbligatoria l'innovazione nella pubblica amministrazione nel modo più naturale: da una parte, dando ai cittadini diritti e strumenti per interagire sempre, dovunque e verso qualsiasi amministrazione attraverso Internet, posta elettronica, reti; dall'altra, stabilendo che tutte le amministrazioni devono organizzarsi per rendere disponibili tutte le informazioni e tutti i procedimenti in modalità digitale, sempre e comunque.

Vengono inoltre introdotte misure premiali e sanzionatorie, consentendo alle pubbliche amministrazioni di quantificare e riutilizzare i risparmi ottenuti grazie alle tecnologie digitali. Dalla razionalizzazione della propria organizzazione e dall'informatizzazione dei procedimenti, le pubbliche amministrazioni ricaveranno infatti risparmi da utilizzare per l'incentivazione del personale coinvolto e per il finanziamento di progetti di innovazione. Nel processo di riforma ed innovazione, le amministrazioni sono accompagnate da DigitPA che metterà a disposizione le proprie competenze tecniche per avviare azioni di assistenza tecnica mirata, formazione e consulenza.

Grazie al nuovo CAD, la pubblica amministrazione sarà completamente digitale e sburocratizzata, rendendo al passo con i tempi il quadro normativo e regolatorio mediante il quale ottenere quel recupero di efficienza delle pubbliche amministrazioni, essenziale per dare maggiore impulso al processo di sviluppo del Paese.

Renato Brunetta

| INTRODUZIONE E STRUTTURA DEL MANUALE |

Il 25 gennaio 2011 è entrato in vigore il nuovo CAD, il Codice dell'Amministrazione Digitale (Decreto legislativo n. 235/2010).

Pubblicato sulla Gazzetta Ufficiale del 10 gennaio 2011, n. 6, il nuovo CAD rappresenta il secondo pilastro su cui si basa il processo di rinnovamento della pubblica amministrazione avviato con l'approvazione del Decreto legislativo n. 150/2009 (la cosiddetta "riforma Brunetta") che ha introdotto nella PA principi di meritocrazia, premialità, trasparenza e responsabilizzazione dei dirigenti.

Il nuovo CAD rinnova il quadro normativo in materia di amministrazione digitale definito nel 2005 con il Decreto legislativo n. 82, da un lato, aggiornando le regole rispetto a un panorama tecnologico che in cinque anni ha subito profondi cambiamenti e, dall'altro, dando forma ed effettività a quell'universo di principi e regole che hanno segnato il percorso di trasformazione, rinnovamento in atto da qualche anno nella PA e nell'intero Paese.

Introdotto nel 2005 nel quadro normativo, il CAD ha segnato un'importante svolta nella vita delle amministrazioni pubbliche e nei rapporti di queste con i cittadini e le imprese. Per la prima volta veniva infatti sancito da una legge sia il diritto dei cittadini di relazionarsi con le amministrazioni pubbliche attraverso le tecnologie telematiche (ossia attraverso Internet e il computer), sia l'obbligo per le amministrazioni di attrezzarsi in conseguenza in modo da rendere effettivamente esigibili i nuovi diritti.

È tuttavia evidente che parte delle previsioni allora formulate è stata disattesa. Molto è certamente dipeso dalle difficoltà legate all'applicazione di una legge che spesso si era limitata a enunciare solo dei principi. La necessità di attribuire maggiore incisività alle prescrizioni normative, oltre che di dare risposte al rapido mutamento tecnologico produttivo dell'ultimo quinquennio, richiedeva dunque un aggiornamento del quadro regolatorio.

Il nuovo Codice dell'Amministrazione Digitale costituisce un insieme organico di norme che si pone l'obiettivo di creare le condizioni giuridiche e organizzative perché si possa finalmente completare il passaggio da un'amministrazione basata su carta e sul riconoscimento *de visu* dei cittadini ad una "amministrazione digitale" (come alcuni direbbero, una "amministrazione web 2.0"), ispirata a modelli operativi e strumenti di comunicazione in grado di sfruttare appieno i vantaggi e le potenzialità offerte dalle nuove tecnologie.

In questo quadro, disporre di indicazioni chiare sulla validità e sull'efficacia probatoria del documento elettronico - nonché far riferimento a specifiche regole tecniche per la formazione, tenuta e conservazione del documento stesso - rappresentano le condizioni essenziali per rendere effettivo il passaggio dalla carta al digitale.

Il nuovo CAD risponde a queste esigenze di effettività, facendo in modo che sia diritto dei cittadini usufruire di servizi digitali da parte della PA e imponendo alle strutture pubbliche alcune regole chiave su come ottemperare alla nuova domanda senza incertezze e dubbi interpretativi.

Esigibilità dei diritti per cittadini e imprese: i cittadini e le imprese hanno diritto di usare le tecnologie informatiche per tutti i rapporti con qualsiasi amministrazione pubblica. Quindi per un'amministrazione non è più possibile obbligare i cittadini a recarsi agli sportelli per presentare documenti cartacei, per firmare 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. Il nuovo Codice amplia questo diritto anche verso i gestori di servizi pubblici. Il complesso della riforma della PA permette poi di esigere questo diritto anche mediante l'uso dell'azione collettiva (*class action*) e introduce l'effettiva disponibilità degli strumenti necessari nella valutazione dei dirigenti e delle organizzazioni.

Chiarezza, validità giuridica e sicurezza: il CAD dissipa molte incertezze, chiarisce dubbi di validità e di effettiva valenza probatoria dei documenti informatici, rassicura gli operatori, indica strumenti concreti e disponibili. Ancora, attraverso una maggiore apertura al mercato, crea le condizioni per un'innovazione diffusa, spinta dalla domanda e sostenuta da un'offerta qualificata e consapevole. Il Codice, inoltre, fa chiarezza sulle molte opportunità che il nuovo assetto regolatorio offre alle PA.

Valutazione e premialità: i risultati delle PA dovranno essere effettivamente misurati e andranno in parte ad incentivare il personale interessato (secondo le norme del Decreto legislativo n.150/2009), in parte a finanziare nuova innovazione.

Risparmi concreti: il CAD prevede che le pubbliche amministrazioni potranno utilizzare i risparmi derivanti dalla razionalizzazione della propria organizzazione e dall'informatizzazione dei procedimenti per l'incentivazione del personale coinvolto e per il finanziamento di progetti di innovazione.

I cambiamenti descritti non avverranno in un giorno. L'azione riformatrice è strutturata in modo da consentire alle amministrazioni di realizzare gli interventi necessari in un tempo ragionevole, utilizzando al meglio le risorse disponibili.

In coerenza con il Piano e-Gov, l'orizzonte temporale dell'intervento è il 2012. Entro i prossimi 18 mesi, famiglie e imprese potranno colloquiare attraverso computer e Internet con tutte le amministrazioni locali e centrali.

Entro i prossimi 18 mesi diverrà dunque concreto e operativo il grande progetto della pubblica amministrazione digitale impostato nel 2005.

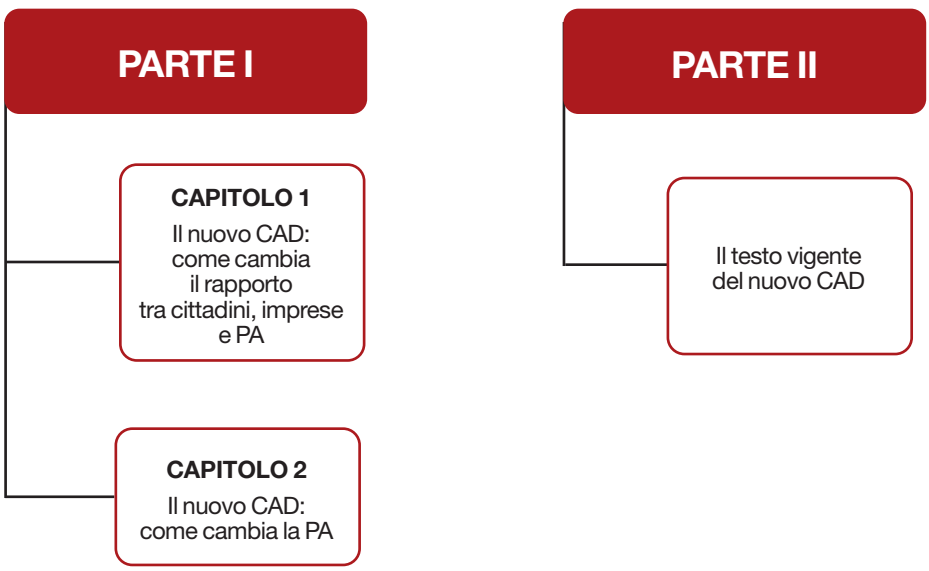
Questo Manuale, strutturato in due parti, vuole essere una "guida alla lettura" del nuovo Codice (Schema 1).

La prima parte è suddivisa in due Capitoli.
Il Capitolo 1 si rivolge a cittadini e imprese. Ripercorrendo il ciclo del documento digitale, il Capitolo descrive i diritti di cittadini e imprese nei confronti dell'amministrazione digitale. In particolare, sono illustrati gli strumenti che consentono, attraverso l'uso delle tecnologie informatiche, di interagire con amministrazioni pubbliche e gestori di servizi pubblici (art. 3), che non possono più pretendere che i cittadini debbano recarsi fisicamente agli sportelli per presentare documenti cartacei, firmare istanze, fornire o richiedere chiarimenti *de visu*.

Il Capitolo 2 è diretto alle pubbliche amministrazioni e presenta le opportunità e i doveri per la PA che discendono dall'introduzione del nuovo CAD. Dal momento che tutte le PA devono attrezzarsi per disporre di un canale digitale sicuro (spesso costituito dalla PEC), certificato e con piena validità giuridica in modo da consentire a cittadini e imprese di dialogare dal proprio computer con gli uffici pubblici, il Capitolo richiama i principali cambiamenti organizzativi che la PA è chiamata a realizzare per il passaggio da un'amministrazione cartacea a una digitale.

La seconda parte contiene il testo del CAD (Decreto legislativo n. 82/2005) coordinato e aggiornato con le modifiche e integrazioni introdotte dal Decreto legislativo n. 235/2010.

Schema 1 – Struttura e contenuti del Manuale



PARTE I

Il nuovo CAD: regole, cambiamenti e opportunità

|CAP. I| IL NUOVO CAD: COME CAMBIA IL RAPPORTO TRA CITTADINI, IMPRESE E PA

|INTRODUZIONE|

Questo Capitolo ripercorre le principali novità introdotte dal Codice dell'Amministrazione Digitale a favore di cittadini e imprese, spiegando gli effetti che esse producono nella prassi quotidiana e mettendo in luce il cambiamento che da esse deriva nei rapporti con la PA:

1) la prima sezione focalizza l'attenzione sul documento digitale, chiarendone sinteticamente caratteristiche, condizioni di validità e modalità di impiego;
2) la seconda sezione spiega la trasformazione che il CAD genera in base agli strumenti e alle regole per l'identificazione on line, sui processi di comunicazione e di interazione con la PA digitale.

Una visione di sintesi del Capitolo è offerta nello Schema 2, che illustra le principali novità introdotte dal CAD per cittadini e imprese.

Schema 2 – Le principali novità introdotte dal CAD per cittadini e imprese

SEZIONE 1
Il documento digitale e le regole per la sua validità

Il "ciclo del documento digitale": che cos'è, quando è valido, come si utilizza

Le regole per la validità del documento digitale

Validità dei documenti indipendentemente dal supporto (artt. 20-23 quater): Il nuovo CAD introduce un sistema di regole per sancire la conformità dei documenti cartacei a quelli digitali.

Validità delle copie e dei duplicati (artt. 22, 23, 23-bis): Il nuovo CAD fornisce indicazioni sulla validità delle copie informatiche di documenti con riferimento preciso circa le diverse possibilità (copia digitale del documento cartaceo, duplicazione digitale, ecc.).

SEZIONE 2
Interazione con la PA digitale e regole di identificazione on line

Firme (artt. 1, comma 1, lett. q-bis e 28, comma 3-bis): si introduce il concetto di firma elettronica avanzata, con cui è possibile sottoscrivere un documento informatico con piena validità legale; si amplia il mercato delle firme digitali, prevedendo che le informazioni relative al titolare e ai limiti d'uso siano contenute in un separato certificato elettronico e rese disponibili anche in rete.

Posta elettronica certificata (artt. 6 e 65): la PEC diventa il mezzo più veloce, sicuro e valido per comunicare con le PA. I cittadini possono utilizzare la PEC anche come strumento di identificazione. La stessa validità è estesa alle trasmissioni effettuate tramite PEC che rispettano i requisiti tecnici. Le istanze possono essere trasmesse da tutte le caselle di posta elettronica certificata rilasciate previa identificazione del titolare.

Carta d'identità elettronica e Carta nazionale dei servizi (art. 64): strumenti validi ai fini dell'identificazione elettronica.

Accesso ai servizi in rete (art. 64): per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni è possibile utilizzare anche strumenti diversi dalla Carta d'identità elettronica e dalla Carta nazionale dei servizi, previa individuazione del soggetto che ne richiede il servizio.

Trasmissione delle informazioni via web (art. 58): le pubbliche amministrazioni non possono richiedere informazioni di cui già dispongono. Per evitare che il cittadino debba fornire più volte gli stessi dati, le amministrazioni titolari di banche dati predisporranno apposite convenzioni aperte per assicurare l'accessibilità delle informazioni in proprio possesso da parte delle altre amministrazioni.

Comunicazioni tra imprese e amministrazioni (art. 5 - bis): la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti (anche a fini statistici) tra imprese e PA (e viceversa) avviene solo utilizzando tecnologie ICT.

Customer satisfaction dei cittadini su internet (art. 63): le pubbliche amministrazioni sono tenute ad adottare strumenti idonei alla rilevazione immediata, continua e sicura del giudizio dei propri "clienti" sui servizi on line.

|2| IL DOCUMENTO DIGITALE: CHE COS'È E QUANDO È VALIDO

Il punto di partenza per il processo di dematerializzazione delle comunicazioni (con la pubblica amministrazione, ma anche tra privati) è il documento digitale: il nuovo Codice traccia la via per la piena equiparazione del documento cartaceo a quello informatico, delineando in modo chiaro rispetto al passato i requisiti e le regole essenziali per la validità del documento digitale, anche rispetto alle situazioni in cui un documento subisca la conversione, da analogico a digitale o viceversa.

|2.1| Definizione e condizioni di validità

Un documento digitale può avere origini di diverso tipo. Infatti, è possibile:

1. creare direttamente un atto in formato digitale elettronico;
2. trasformare in digitale un documento originariamente creato in formato analogico (ossia cartaceo).

Secondo l'art. 20, il documento informatico formato da chiunque, memorizzato su supporto informatico e trasmesso con strumenti telematici, conformemente alle regole tecniche esistenti e alle integrazioni che saranno emanate entro dodici mesi[1], ha la stessa validità, ad ogni effetto di legge, del documento cartaceo e deve essere accettato da qualsiasi soggetto pubblico o privato (Schema 3).

In base al nuovo Codice, un documento informatico:

- è liberamente valutabile in giudizio se firmato con firma elettronica semplice;
- è pienamente valido, come una qualsiasi sottoscrizione riconosciuta (art. 2702 c.c.), se firmato con firma avanzata, qualificata o digitale;
- è pienamente valido solo se firmato con firma qualificata o digitale nel caso si tratti di una scrittura privata di particolare rilevanza (art. 1350 c.c. comma 1 – numeri da 1 a 12), come ad esempio una compravendita di immobili.

[1] L'art. 20 comma 3 chiarisce che le regole tecniche per la formazione, la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica avanzata delle firme elettroniche, salvo quanto già disposto in materia di firma digitale, saranno adottate entro il 25 gennaio 2012 (dodici mesi dall'entrata in vigore del nuovo CAD). La legge riconosce inoltre validità giuridica all'attestazione di data e all'ora se apposte in conformità alle citate regole tecniche sulla validazione temporale. Tali regole saranno emanate con decreto del presidente del Consiglio dei Ministri o del ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il ministro per i beni e le attività culturali e la Conferenza unificata, sentiti DigitPA e il Garante per la protezione dei dati personali. Tali norme daranno piena effettività al processo di dematerializzazione dei documenti della PA.

Schema 3 - La validità del documento informatico	
Documento informatico provvisto di forma elettronica semplice	• È liberamente valutabile in giudizio.
Documento informatico cui viene apposta firma elettronica avanzata, qualificata o digitale	• Costituisce piena prova fino a querela di falso.
Documento informatico contenente una delle scritture private individuate dall'art. 1350 c.c. *comma 1 – numeri da 1 a 12* (esempio: contratti di locazione di beni immobili con durata superiore a 9 anni; usufrutto; contratti di società per il conferimento di beni per l'esercizio dell'attività economica; ecc.)	• Costituisce piena prova fino a querela di falso e, a pena nullità, richiede la firma elettronica qualificata o digitale.

Il Codice chiarisce inoltre il valore giuridico della copia dei documenti informatici (Schema 4), a seconda che ci si trovi in una delle situazioni di seguito descritte:

- **copia informatica di un documento cartaceo analogico (art. 22 comma 1)**: un documento informatico che è copia informatica di un documento cartaceo[2] (per esempio un atto pubblico, una scrittura privata e un documento amministrativo) è valido se spedito o rilasciato da depositari pubblici autorizzati o da pubblici ufficiali e firmato con firma digitale o qualificata;
- **copia per immagine su supporto informatico di documento cartaceo (art. 22 commi 2 e 3)**: ad esempio, nel caso in cui, mediante scanner, si ottiene un nuovo documento informatico formato dalle immagini di un documento su carta. Tale copia:
  - è valida, se la conformità è attestata da un notaio o da un pubblico ufficiale autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche (art. 22 comma 2);
  - ha comunque la stessa efficacia dell'originale, nel rispetto delle regole tecniche[3], se non è espressamente disconosciuta (art. 22 comma 3);
- **copia analogica di un documento informatico (art. 23)**:
  - una copia su supporto analogico di un documento informatico (anche sottoscritta con firma avanzata qualificata o digitale) è pienamente valida se la conformità all'originale è attestata da un pubblico ufficiale autorizzato (art. 23 comma 1);

[2] Si sostituisce per chiarezza "analogico" con "cartaceo" perché, seppur diversi, nel contesto pratico della documentazione della PA i due termini possono essere considerati equivalenti.
[3] Tali regole tecniche saranno emanate entro 12 mesi dall'entrata in vigore del nuovo CAD.

- una copia cartacea di un documento informatico, se conforme alle regole tecniche, ha comunque la stessa efficacia probatoria dell'originale se la conformità non è espressamente disconosciuta. Lo stesso dicasi per gli estratti su supporto analogico del documento informatico (art. 23 comma 2);

- **copia informatica di un documento informatico (art. 23-bis comma 2)**: un documento il cui contenuto è lo stesso dell'originale, ma con una diversa sequenza di valori binari rispetto al documento originario (come quando si trasforma un documento .doc in un documento .pdf). Tale copia, prodotta in conformità alle regole tecniche, ha lo stesso valore probatorio dell'originale da cui ha origine, se un pubblico ufficiale autorizzato ne attesta la conformità oppure se la stessa conformità non viene espressamente disconosciuta. Lo stesso dicasi per gli estratti.

Il Codice stabilisce inoltre il valore giuridico del "**duplicato**" (Schema 4):

- **duplicato informatico di un documento informatico (art. 23-bis comma 1)**: se prodotto in conformità con le regole tecniche, un documento informatico – ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario (come quando si copia un documento nel medesimo formato su un supporto diverso, ad esempio dal PC a una pen-drive) – ha lo stesso valore giuridico del documento informatico da cui è tratto.

Schema 4 - La validità di copie e duplicati

Copia informatica di documento cartaceo	• Se proviene da depositari pubblici autorizzati o da pubblici ufficiali. • Se presenta la firma digitale o altra firma elettronica qualificata del soggetto che rilasci a la copia.
Copia per immagine su supporto informatico di un documento cartaceo (esempio: scansione del documento)	• Se la sua conformità al documento originale è attestata da un notaio o da altro pubblico ufficiale autorizzato.
Copie cartacee di documento informatico	• Se la sua conformità all'originale, in tutte le sue componenti, è attestata da un pubblico ufficiale.
Copia informatica del documento informatico	• Ha l'efficacia probatoria dell'originale da cui è tratta, se si verifica una delle seguenti condizioni. • La sua conformità all'originale è attestata da un pubblico ufficiale a ciò autorizzato. • La conformità all'originale non è espressamente disconosciuta.
Duplicato informatico	• Ha il medesimo valore giuridico del documento informatico da cui è tratto.

È opportuno far presente che nel Capitolo 2, dedicato alle pubbliche amministrazioni, verrà descritta una ulteriore tipologia di documento informatico: **il documento amministrativo informatico** (par. 2.1). L'art. 23-ter del nuovo CAD trasla alla pubblica amministrazione i principi appena richiamati e, in più, introduce il cosiddetto "timbro elettronico" (comma 5), ossia un contrassegno generato elettronicamente diretto ad assicurare – se rispettate determinate regole tecniche – la provenienza e la conformità all'originale.

|2.2| Le firme elettroniche

La validità dei documenti informatici è dunque strettamente connessa con la questione della "sottoscrizione elettronica" dei documenti. Così come accade per i documenti cartacei, infatti, la sottoscrizione permette di attribuire all'autore la paternità giuridica di un documento informatico.

Il sistema delle firme elettroniche trova oggi nel Codice un nuovo assetto e una nuova organizzazione derivata soprattutto dall'introduzione, in coerenza con le norme comunitarie, della firma elettronica avanzata che, introdotta nel 2000, era stata poi abolita dalla versione del Codice del 2005.

Lo Schema 5 descrive – sulla base di quanto previsto dal Codice – le diverse firme elettroniche, le loro caratteristiche e il relativo valore giuridico tenendo conto che esse, nel passaggio dalle firme cosiddette deboli a quelle definite forti, garantiscono maggiore sicurezza sull'autore di un documento digitale:

- le cosiddette ***firme deboli*** (firma elettronica) consentono di ricondurre in qualsiasi forma dei dati elettronici, ad esempio una firma a stampa, ad un soggetto, ma non assicurano l'integrità del documento stesso. Il documento è liberamente valutabile in giudizio, tenendo conto delle sue caratteristiche oggettive di qualità e sicurezza;
- le cosiddette ***firme forti*** (firma elettronica avanzata, firma elettronica qualificata e firma digitale) sono quelle per cui il firmatario non può disconoscere semplicemente la sottoscrizione se non a querela di falso. Garantiscono l'identità dell'autore e l'integrità del documento firmato.

Si ricorda inoltre la ***firma elettronica autenticata*** secondo l'art. 25 del CAD. L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione da parte del pubblico ufficiale (ad esempio, un notaio) che la firma è stata apposta in sua presenza dal titolare - previo accertamento della sua identità personale - della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico. L'apposizione della firma digitale da parte del pubblico ufficiale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente. Questa firma è equiparata, ai fini di legge, alla sottoscrizione autenticata dal notaio o da altro pubblico ufficiale. Si tratta del procedimento di firma considerato in assoluto più sicuro.

Schema 5 - Le firme elettroniche	
Firme deboli	
Firma elettronica	Con l'espressione firma elettronica (c.d. firma debole) si intende un insieme di dati in forma elettronica, riconducibili all'autore (anche di tipo: log identificativo, indirizzo mail, ecc.), allegati oppure connessi ad atti o fatti giuridicamente rilevanti contenuti in un documento informatico. La firma elettronica offre minori requisiti di sicurezza rispetto alle altre firme (c.d. forti).
Valore giuridico: la normativa riconosce alla firma elettronica un valore probatorio. La firma è liberamente valutata dal giudice in fase di giudizio, in base a caratteristiche oggettive di qualità e sicurezza.	
Firme forti	
Firma elettronica avanzata	È un particolare tipo di firma elettronica che, allegando oppure connettendo un insieme di dati in forma elettronica ad un documento informatico, garantisce integrità (consentendo di rilevare se i dati sono stati successivamente modificati), autenticità del documento sottoscritto e controllo esclusivo dello strumento di firma. Quest'ultimo elemento assicura la connessione univoca con il firmatario e quindi la paternità giuridica del documento. Si tratta di una tipologia di firma prevista dal Codice, ma che (ad oggi) non è ancora disponibile in quanto la regolamentazione tecnica è affidata ad un decreto che dovrà essere emanato dal Governo entro 12 mesi dall'entrata in vigore del nuovo CAD.
Valore giuridico: Il documento informatico sottoscritto con firma elettronica avanzata, formato nel rispetto delle regole tecniche, è riconosciuto valido fino a querela di falso. Quindi, questa tipologia di firma comporta l'inversione dell'onere della prova, per cui chi intende disconoscere la sottoscrizione di un documento dovrà provare che l'apposizione della firma è riconducibile ad altri e che tale apposizione non è imputabile a sua colpa.	
Firma elettronica qualificata	È un particolare tipo di firma elettronica avanzata basato su un certificato "qualificato" (che garantisce l'identificazione univoca del titolare, rilasciato da certificatori accreditati) e realizzato mediante un dispositivo sicuro per la generazione della firma (*Secure Signature Creation Device* - SSCD) che soddisfa particolari requisiti di sicurezza. Il certificato può contenere limitazioni relative alla tipologia di atti da sottoscrivere o a tetti di spesa. Gli SSCD disponibili oggi sul mercato sono rappresentati da dispositivi di tipo differente, come, ad esempio, *smart card* e chiave USB, tutti dotati di un chip che consente la generazione di firme elettroniche qualificate esclusivamente al titolare legittimo.
Firma digitale	È un particolare tipo di firma elettronica avanzata basato su un certificato qualificato e su un sistema di doppia chiave crittografica, una pubblica (contenuta nel certificato qualificato, a sua volta contenuto in ogni documento sottoscritto) ed una privata (custodita dal mittente) che, nel loro uso congiunto, servono a garantire e a verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. Non è, invece, contemplato l'obbligo di utilizzo dell'SSCD. Come per la firma avanzata, anche per la firma digitale la regolamentazione tecnica è affidata ad un decreto che dovrà essere emanato dal Governo entro 12 mesi dall'entrata in vigore del nuovo CAD.
Valore giuridico: Il documento informatico sottoscritto con firma elettronica qualificata o firma digitale, formato nel rispetto delle regole tecniche, è riconosciuto valido a tutti gli effetti di legge e soddisfa il requisito della forma scritta, secondo quanto previsto dall'art 1350 c.c., punti 1-12. Le elevate garanzie di sicurezza connesse comportano, anche per queste tipologie di firme, l'inversione dell'onere della prova, per cui chi intende disconoscere la sottoscrizione di un documento dovrà provare che l'apposizione della firma è riconducibile ad altri e che detta apposizione non è imputabile a sua colpa. La firma digitale [4], ante modifiche al CAD, corrisponde alla firma elettronica qualificata che utilizza la crittografia a chiave pubblica.	

[4] Le operazioni da compiere per apporre la firma ad un file possono variare in base al software di firma utilizzato. I tratti fondamentali, però, sono comuni a tutti gli applicativi utilizzati. Il software di firma chiederà di selezionare il documento da sottoscrivere e di inserire la smart card o chiavetta USB nel lettore o porta USB. Successivamente il software chiederà l'inserimento del codice PIN e salverà un file sottoscritto e pronto per essere utilizzato. I formati di firma consentiti sono tre: CAdES, PAdES e XAdES.

|3| L'USO DEL DOCUMENTO DIGITALE NEI RAPPORTI CON LA PA

In che modo il documento digitale cambia le modalità di comunicazione e di interazione tra cittadino e PA?

Il Codice, all'art. 3, riconosce un vero e proprio diritto in capo a cittadini e imprese all'utilizzo delle moderne tecnologie informatiche per tutti i rapporti con le amministrazioni cui si applica la normativa sul pubblico impiego[5], alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico e ai gestori di pubblici servizi. Le amministrazioni e i gestori di pubblico servizio non possono più pretendere che i cittadini si rechino presso gli uffici per il disbrigo delle pratiche (presentazione di documenti cartacei, sottoscrizione di richieste e istanze, ecc.).

Il nuovo Codice ha previsto un'ulteriore specificazione di questo principio: secondo l'art. 5-bis, i rapporti tra le PA e le imprese dovranno avvenire esclusivamente per via telematica. Ciò vale sia nel caso in cui è l'impresa a presentare istanze e dichiarazioni, sia quando le PA adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese. L'implementazione di questo canale esclusivo di comunicazione è demandata ad un decreto della Presidenza del Consiglio dei Ministri (da emanarsi entro 6 mesi dall'entrata in vigore del nuovo Codice) con cui saranno adottate le modalità di attuazione da parte delle pubbliche amministrazioni centrali e fissati i relativi termini.

Affinché ciò si realizzi nella prassi quotidiana, quali sono le condizioni necessarie per cui cittadini e imprese possono esercitare il diritto a comunicare "in digitale" con la PA? Il Codice precisa che l'invio di documenti ad una pubblica amministrazione attraverso qualsiasi mezzo telematico o informatico che permetta di accertare la fonte di provenienza soddisfa il requisito della forma scritta e non è, quindi, necessario che l'invio sia seguito dalla produzione del documento originale[6].

Più specificamente, il Codice ridefinisce anche parte dei parametri per la validità delle istanze e delle dichiarazioni presentate alle pubbliche amministrazioni per via te-

La firma CAdES è applicabile a qualunque file cui, a seguito dell'apposizione della firma, pur conservando il nome e l'estensione originale ,è aggiunta l'estensione della firma applicata (.p7m" (es. Contratto.rtf.p7m.) Il formato PAdES è relativo alla firma contenuta nei file PDF, il formato XAdES ai file XML. A questi ultimi due nessuna estensione è aggiunta conseguentemente all'applicazione della firma. Nel caso in cui il processo di firma interessi un numero elevato di documenti è possibile automatizzare le procedure di sottoscrizione purché l'operazione di firma automatizzata si svolga nel rispetto della normativa tecnica vigente.

[5] 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 montane e loro consorzi e 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 (secondo la nota enumerazione contenuta nell'art. 1, comma 2, del Decreto Legislativo 30 marzo 2001, n. 165).

[6] Questo principio trova conferma anche nell'art. 38 comma 2 del DPR 445/2000 alla luce del quale le istanze e le dichiarazioni inviate per via telematica, comprese le domande per la partecipazione a selezioni e concorsi o per l'iscrizione in albi, registri o elenchi tenuti presso le pubbliche amministrazioni, sono valide se effettuate nel rispetto delle modalità individuate dall'art. 65 del nuovo Codice.

lematica (art. 65). Queste richieste sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa dal richiedente apposta in presenza del dipendente addetto al procedimento, se sussiste almeno uno dei seguenti elementi:

- **firma digitale del documento** - la richiesta è sottoscritta mediante la firma digitale, il cui certificato sia stato rilasciato da un certificatore accreditato;
- **copia per immagine non autenticata di un documento di identità valido** - le istanze e le dichiarazioni sono inviate con le modalità prescritte dall'art. 38 comma 3 del DPR 28 dicembre 2000 n. 445, il quale prevede che le istanze e le dichiarazioni sostitutive di atto di notorietà rivolte alla amministrazione pubblica (o ai gestori o esercenti di pubblici servizi) possono essere sottoscritte e presentate allegando una copia (acquisita sotto forma di immagine, come nel caso della scansione della Carta d'identità) non autenticata di un documento di identità valido;
- **identificazione certa dell'autore** - l'autore è identificato dal sistema informatico attraverso
  1) la **Carta d'Identità Elettronica (CIE)** o la **Carta Nazionale dei Servizi (CNS)**[7];
  2) i diversi strumenti predisposti dalle amministrazioni che consentano l'**individuazione del soggetto che richiede il servizio** (ad esempio: pin e password);
  3) la **Posta Elettronica Certificata (PEC)**: la richiesta è trasmessa dall'autore mediante la propria casella PEC, purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare anche per via telematica secondo modalità definite con apposite regole tecniche[8] (adottate entro 12 mesi dall'entrata in vigore del nuovo CAD) e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato[9].

|3.1| La PEC per comunicare con la PA digitale

Nel modello disegnato dal Codice, la PEC assume un ruolo centrale nelle comunicazioni tra i privati e la pubblica amministrazione.

La PEC è un servizio che somma alle comuni funzioni di posta elettronica funzionalità in grado di fornire certezza sulle identità del mittente e del destinatario, sull'ora di invio e di consegna e sull'integrità del messaggio inviato. La PEC garantisce al mittente l'attestazione, con valenza legale, dell'invio e della consegna (o mancata consegna) di documenti informatici. Nel momento in cui il messaggio viene recapitato nella casella di posta del destinatario, il gestore del sistema invia al mittente una ricevuta, firmata digitalmente, che certifica questi dati. In questo modo l'utilizzo della PEC viene equiparato, ad ogni effetto di legge, alla notifica a mezzo posta (raccomandata A/R).

[7] La Carta d'Identità Elettronica è il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare. La Carta Nazionale dei Servizi è il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni.

[8] Tali regole tecniche saranno adottate entro 12 mesi dall'entrata in vigore del nuovo CAD.

[9] Restano, comunque, salve le norme che prevedono l'uso di sistemi specifici di trasmissione telematica nel settore tributario.

Prima dell'entrata in vigore del nuovo Codice, l'ordinamento aveva già, in più momenti, considerato la PEC come un mezzo valido e sicuro per le comunicazioni con le amministrazioni pubbliche (Schema 6).

Schema 6 – PEC: evoluzione del quadro normativo

La PEC nel CAD 2005	Il Codice dell'Amministrazione Digitale, già nella sua formulazione originaria, individuava nella posta certificata uno strumento privilegiato per ogni scambio di documenti e informazioni tra le PA e i soggetti interessati che richiedevano l'utilizzo di questo canale di comunicazione. Si esortava, inoltre, l'amministrazione a comunicare con i propri dipendenti usando la posta elettronica. Successivamente sono intervenute altre norme che hanno ampliato la portata giuridica della PEC nei rapporti tra i privati e le amministrazioni.
La Legge n. 2/2009	Con la Legge n. 2/2009 il legislatore ha introdotto l'obbligo per le pubbliche amministrazioni di istituire e pubblicare almeno una casella di posta elettronica certificata, per ciascun registro di protocollo, sull'apposito indice delle pubbliche amministrazioni (IPA) gestito da DigitPA. Le amministrazioni inoltre hanno l'obbligo di pubblicare sulla pagina iniziale del proprio sito istituzionale l'indirizzo PEC, al fine di consentire al cittadino l'inoltro di richieste in modalità telematica. Con l'obiettivo di semplificare il rapporto tra cittadino e PA, il legislatore ha previsto la creazione di un canale diretto di comunicazione digitale per i cittadini, offrendo a questi ultimi la possibilità di richiedere una casella di posta elettronica certificata gratuita (servizio postacertificat@: www.postacertificata.gov.it). La pubblicazione delle PEC sull'indice IPA è strumentale per l'interoperabilità tra il circuito postacertificat@ e le PEC acquistate sul mercato. Al fine di facilitare la ricerca degli indirizzi PEC delle amministrazioni pubblicate sull'indice IPA da parte di cittadini, imprese, liberi professionisti, inoltre è stato attivato un motore di ricerca denominato "paginepecpa" (www.paginepecpa.gov.it). Infine, la norma citata ha introdotto l'obbligo anche per professionisti[10] e imprese[11] di dotarsi di un indirizzo PEC.

Il nuovo Codice definisce il quadro giuridico di riferimento complessivo sull'uso della posta elettronica certificata intesa come strumento di identificazione più veloce, sicuro e legalmente valido per comunicare tra i privati e le amministrazioni pubbliche, anche senza l'uso della firma digitale.

Il CAD ribadisce che il cittadino-cliente che dialoga via PEC ha diritto a risposte con lo

[10] Entro il 29 novembre 2009.

[11] Con scadenze diverse a seconda che si tratti di nuove imprese o di imprese già esistenti (in quest'ultimo caso, il termine previsto è il 29 novembre 2011).

stesso mezzo. Le amministrazioni, infatti, sono tenute a (cfr. Capitolo 2):

- utilizzare la PEC per tutte le comunicazioni che necessitano di una ricevuta di invio e di consegna con i soggetti che hanno preventivamente dichiarato il proprio indirizzo PEC (art. 6, comma 1);
- accettare e dare seguito alle istanze che pervengono via PEC, in quanto equiparate alle dichiarazioni che il richiedente firma in presenza del dipendente addetto al procedimento (art. 65, comma 1 c-bis)[12].

Un documento inviato tramite PEC ha quindi valore legale, anche in assenza di firma digitale, nel rispetto delle condizioni prima richiamate in merito al rilascio delle credenziali di accesso, all'identificazione del titolare e alla relativa attestazione da parte del gestore del sistema nel messaggio o in un suo allegato. Restano in vigore le norme che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario.

Inoltre, a seguito della riforma, la PEC può essere utilizzata anche per l'invio della diffida all'amministrazione o al concessionario di pubblico servizio, richiesta dalla legge, per l'avvio del ricorso collettivo per l'efficienza delle amministrazioni e dei concessionari di servizi pubblici (la cosiddetta azione collettiva; cfr. par. 5)[13].

L'insieme di obblighi ed opportunità sono sintetizzati nello Schema 7.

Schema 7 - La PEC: obblighi e opportunità per cittadini, imprese e professionisti

La PEC per i cittadini	
Firma elettronica	• Beneficiare della casella di posta gratuita del circuito postacertificat@ per il dialogo e i rapporti con la PA. • Utilizzare l'indirizzo PEC, dichiarato alle PA, come canale privilegiato di comunicazione. • Presentare validamente istanze e dichiarazioni alla PA per via telematica senza necessità di sottoscrivere digitalmente richieste e file allegati, a condizione che l'identificazione del titolare sia attestata dal gestore.
La PEC per imprese e professionisti	
Obblighi	• Istituire un indirizzo PEC e comunicarlo al proprio Ordine professionale o al Registro delle imprese.
Opportunità	• Disponibilità di uno strumento veloce e sicuro per ottimizzare i rapporti con la PA e i soggetti privati.

[12] Rispetto alla tipologia di richieste che possono essere veicolate attraverso la PEC, il Codice non pone particolari limiti. Tuttavia si fa presente che il Ministro per la pubblica amministrazione e l'innovazione e il Ministro per la semplificazione normativa, su proposta dei Ministri competenti per materia, potranno individuare, attraverso un decreto, i casi in cui è necessaria la sottoscrizione mediante firma digitale (art. 65, comma 1-bis).

[13] Da ultimo, il Codice dettaglia il potere sanzionatorio, in capo a DigitPA, nei confronti dei gestori di PEC accreditati: in caso di malfunzionamenti che determinano un disservizio si applicano la diffida o la cancellazione dall'elenco di gestore accreditato (art. 32-bis).

|4| DIRITTO DI ACCESSO E DIRITTO ALLA SICUREZZA

Oltre a sancire il diritto all'utilizzo del canale telematico nei rapporti con la PA, il nuovo CAD riconosce a cittadini e imprese il diritto a partecipare al procedimento amministrativo informatico e di accedere ai documenti amministrativi (art. 4, comma 1), diritto che si estende ad ogni fatto rilevante (ogni atto, documento o procedimento amministrativo) del rapporto tra l'amministrazione e i privati.

L'art. 64 del nuovo CAD, oltre a confermare la validità della Carta di Identità Elettronica (CIE) e della Carta Nazionale dei Servizi (CNS) come mezzi di identificazione per l'accesso ai servizi erogati in rete dalle PA, consente alle amministrazioni di far accedere i cittadini e le imprese ai servizi on line che necessitano di identificazione informatica anche tramite altri strumenti in grado di garantire l'individuazione certa del soggetto che richiede il servizio (come nel caso della PEC).

Inoltre, il nuovo Codice prescrive esplicitamente alle amministrazioni (art. 41) di dar conto ai cittadini dello stato delle pratiche che li riguardano, obbligo per le PA che si aggiunge a quello di raccogliere e digitalizzare tutti gli atti, dati e documenti amministrativi da chiunque formati (protocollo e fascicolo informatico) e di dotare i fascicoli anche di un apposito identificativo che ne favorisca la tracciabilità.

Proprio in questo senso – come vedremo nel Capitolo 2 – e con l'obiettivo di creare una PA efficiente, rapida e sicura, il nuovo CAD fornisce precise indicazioni anche in merito all'archiviazione, alla conservazione e alla sicurezza dei dati, così come impone di adottare misure e soluzioni che proteggano da rischi di perdita di dati o di *default* del sistema (*disaster recovery*).

|5| SE LA PA NON È DIGITALE: AZIONE COLLETTIVA E VALUTAZIONE

Al fine di garantire l'effettività dei diritti richiamati, il Legislatore riconosce la possibilità a cittadini e imprese di ricorrere innanzi al giudice amministrativo per sanzionare il comportamento delle amministrazioni che non mettano a disposizione del pubblico un canale digitale sicuro, certificato e perfettamente valido dal punto di vista giuridico. La tutela giurisdizionale dei diritti legati al dialogo con le amministrazioni e alla partecipazione ai procedimenti con l'ausilio delle nuove tecnologie trova quindi ora un ulteriore strumento di tutela rappresentato dal ricorso collettivo per l'efficienza delle amministrazioni e dei concessionari di servizi pubblici (la cosiddetta azione collettiva).

In coerenza con il quadro normativo il nuovo CAD stabilisce, come vedremo nel Capitolo 2, che le pubbliche amministrazioni che erogano servizi online debbano prevedere strumenti idonei alla rilevazione diretti all'acquisizione immediata del giudizio degli utenti. Si ribadisce così il principio cardine della cosiddetta "riforma Bru-

netta" (Decreto legislativo n.150/2009), ossia l'*empowerment* dei cittadini, che consiste nel dar loro "voce" anche su Internet per esprimere la propria soddisfazione sulla qualità dei servizi delle PA.

|CAP. 2| IL NUOVO CAD: SI TRASFORMA LA PA

|INTRODUZIONE|

Questo Capitolo presenta le principali novità introdotte dal Codice per la PA, facendo luce su quell'insieme di innovazioni che incidono sull'organizzazione, sulla qualità dei servizi offerti ai cittadini e alle imprese, nonché sull'efficienza delle amministrazioni consentendo di lavorare meglio e spendere meno.

I principali elementi innovativi riguardano:

- valutazione e premialità - il nuovo Codice è strettamente collegato al ciclo della performance e alla valutazione del merito introdotti dalla "riforma Brunetta". L'attuazione delle disposizioni del Codice è infatti rilevante ai fini della misurazione e della valutazione della *performance* organizzativa e individuale dei dirigenti. Alle opportunità si accompagnano quindi sia gli incentivi sia le sanzioni. L'innovazione diventa per la prima volta materia di valutazione del personale, da cui dipende la premialità;
- sostenibilità organizzativa - il Codice detta delle regole che tendono a garantire la sostenibilità organizzativa dell'innovazione. In particolare, impone alle amministrazioni centrali (e consiglia alle Regioni e agli Enti locali) di dotarsi di un nuovo ufficio a livello di dirigente generale che abbia un forte compito di coordinamento di tutta l'innovazione tecnologica dell'Ente.

Il Codice affida a DigitPA il compito di supportare la realizzazione di un'amministrazione digitale, accompagnando la PA in questo processo e intervenendo con azioni sia di tipo tecnico (con la predisposizione dei documenti di dettaglio previsti dal CAD: regole tecniche e linee guida), sia di tipo formativo e informativo rivolte alle amministrazioni.

Tale compito si inquadra nel più generale ruolo di DigitPA, individuato dal Decreto Legislativo 177/2009 a supporto del percorso di innovazione della PA, per cui l'Ente mette a disposizione delle amministrazioni le proprie competenze tecniche stipulando accordi quadro per l'offerta di servizi innovativi, formulando pareri sui contratti siglati dalle PA centrali, monitorando i piani ICT delle amministrazioni e pubblicando linee guida sulla qualità dei beni e dei servizi ICT.

Le amministrazioni, dunque, si potranno avvalere anche per l'attuazione del CAD dell'assistenza tecnica di DigitPA che imposterà, sulla base delle esigenze organizzative e tecnologiche di ciascuna amministrazione, specifiche azioni di supporto ed accompagnamento secondo una *roadmap* di assistenza, avviata sin dal momento dell'entrata in vigore del Codice.

Il Capitolo è strutturato in tre parti:

1) la prima sezione focalizza l'attenzione sulle soluzioni tecniche e i procedimenti organizzativi che la PA è chiamata ad adottare al suo interno in risposta ai principali cambiamenti introdotti dal nuovo CAD;
2) la seconda sezione richiama i principi sanciti dal CAD, in base ai quali alla PA è richiesto di ripensare le modalità con cui interagisce e comunica sia con le altre amministrazioni sia con cittadini e imprese;
3) la terza sezione descrive le caratteristiche dei servizi e degli strumenti (di accesso e di identificazione) che la PA digitale deve offrire ai propri "clienti".

Una visione di sintesi del Capitolo è offerta nello Schema 8.

Schema 8 – Le principali novità introdotte dal CAD per cittadini e imprese

SEZIONE 1
La risposta organizzativa della PA

- **Il documento amministrativo informatico**
- **Protocollo informatico, fascicolo elettronico e tracciabilità**
- **Archiviazione e conservazione dei documenti digitali**
  - **Conservazione digitale dei documenti (artt. 43-44 bis):** è prevista la gestione della conservazione dei documenti e del relativo processo da parte di un responsabile della conservazione che si può avvalere di soggetti pubblici o privati che offrono idonee garanzie. Ogni responsabile della conservazione dei documenti negli uffici pubblici può certificare il processo di digitalizzazione e di conservazione servendosi (se vuote) di conservatori accreditati. La norma introduce la figura dei conservatori accreditati, soggetti che ottengono da DigitPA il riconoscimento del possesso dei requisiti di sicurezza e affidabilità per effettuare il processo e la conservazione dei documenti.
- **I dati delle pubbliche amministrazioni**
  - **Open data (artt. 52 e 68):** il nuovo CAD mette in primo piano la responsabilità delle pubbliche amministrazioni nell'aggiornare, divulgare e permettere la valorizzazione dei dati pubblici secondo principi di *open government*. I dati pubblici saranno fruibili e riutilizzabili per la promozione di progetti di elaborazione e diffusione dei dati anche attraverso finanza di progetto.
- **Sistemi e soluzioni tecniche per la sicurezza, la continuità operativa e il disaster recovery**
  - **Sicurezza digitale (art. 51):** il nuovo CAD contiene disposizioni importanti sia sulla continuità operativa sia sul *disaster recovery*. Le pubbliche amministrazioni dovranno predisporre piani di emergenza idonei ad assicurare, in caso di eventi disastrosi, la continuità delle operazioni indispensabili a fornire i servizi e il ritorno alla normale operatività.

SEZIONE 2
Modalità di interazione e comunicazione tra PA e tra PA, cittadini e imprese

- **Le comunicazioni tra le pubbliche amministrazioni: scambio documenti e cooperazione applicativa**
- **Siti web pubblici e trasparenza della pubblica amministrazione**
  - **Siti pubblici e trasparenza (art. 54):** il nuovo CAD arricchisce il contenuto dei siti istituzionali delle amministrazioni prevedendo che sugli stessi siano pubblicati, in modo integrale, anche tutti i bandi di concorso. La norma obbliga le pubbliche amministrazioni ad aggiornare i dati e le notizie che per legge devono essere pubblicati sul proprio sito istituzionale. Anche tale aspetto viene considerato ai fini della valutazione dei dirigenti.

SEZIONE 3
Servizi della PA digitale

- **I servizi in rete, gli stumenti di accesso e di identificazione digitale**
  - **Moduli on line (art. 57):** le pubbliche amministrazioni hanno l'obbligo di pubblicare online l'elenco dei documenti richiesti per procedimento (moduli e formulati validi) e non possono richiedere l'uso di moduli o formulari che non siano stati pubblicati sul web. La mancata pubblicazione è rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti responsabili.
  - **Carta d'Identità Elettronica (CIE) e della Carta Nazionale dei Servizi (CNS)**
  - **PEC**
  - **Pagamenti elettronici (art. 5):** il nuovo CAD specifica le modalità operative rivolte alle amministrazioni per rendere facilmente eseguibili a cittadini e imprese pagamenti elettronici verso PA mediante tecnologia digitale.

|2| IL NUOVO CAD E LA RISPOSTA ORGANIZZATIVA DELLA PA

L'azione riformatrice del nuovo CAD, come già rilevato, rafforza i diritti di cittadini e imprese nei confronti della PA ed obbliga quest'ultima ad accelerare il processo di innovazione e di digitalizzazione delle procedure organizzative interne.

Tale processo, che richiede un'estesa adozione del documento informatico, impone:

- l'utilizzo di strumenti atti a gestire la documentazione digitale (protocollo informatico e fascicolo informatico);
- il rispetto di principi tecnico-organizzativi diretti ad assicurare, mediante le tecnologie dell'informazione e della comunicazione, la fruibilità, la riutilizzabilità e l'aggiornamento continuo degli archivi pubblici, nonché a garantire la sicurezza dei dati e dei sistemi e la continuità operativa.

|2.1| Il documento amministrativo informatico

Il nuovo Codice rende concreto l'obiettivo di una PA senza carta, diradando l'incertezza degli operatori sulle regole di validità del documento digitale: come illustrato nel Capitolo 1, le amministrazioni non possono più esigere che i cittadini si rechino presso gli uffici per la presentazione di atti cartacei, data la piena equiparazione – se soddisfatti i requisiti precedentemente richiamati e in conformità delle regole tecniche vigenti – del documento digitale a quello analogico.

In aggiunta a quanto già presentato circa la validità dei documenti digitali, occorre tenere presente che il legislatore detta regole specifiche riguardanti i documenti amministrativi informatici (Schema 9), ovvero gli atti prodotti dalle pubbliche amministrazioni con strumenti informatici (compresi i dati e i documenti informatici detenuti dalle PA), stabilendo all'art. 23-ter che:

1. essi costituiscono informazione primaria e originale da cui è possibile, con i requisiti richiamati nel Capitolo 1, effettuare copie e duplicati validi;
2. per essi valgono tutte le condizioni precedentemente indicate per i documenti informatici;
3. le regole tecniche relative alla formazione e alla conservazione di questi particolari documenti informatici, in quanto atti pubblici, saranno definite entro 12 mesi dall'entrata in vigore del nuovo CAD con decreto del presidente del Consiglio dei Ministri o del ministro delegato per la pubblica amministrazione e l'innovazione di concerto con il ministro per i beni e le attività culturali, e d'intesa con la Conferenza Unificata, sentiti DigitPA e il garante per la protezione dei dati personali.

In più, il comma 5 fa chiarezza sulle condizioni per garantire provenienza e conformità all'originale cartaceo di un documento amministrativo digitale introducendo un elemento innovativo, il cosiddetto timbro elettronico: la copia analogica di documenti informatici vede assicurata la provenienza e la conformità con l'originale se vi è ap-

posto a stampa – con criteri definiti con linee guida emanate da DigitPA - un contrassegno generato elettronicamente secondo le regole tecniche di cui al punto 3, e tale da consentire la verifica automatica della conformità tra documento cartaceo e quello informatico (il glifo o timbro elettronico).

Schema 9 - La validità del documento amministrativo informatico

Documento amministrativo informatico	• Costituisce informazione originale da cui è possibile effettuare, nel rispetto della regolamentazione tecnica, copie e duplicati validi. • È sottoposto alle stesse regole stabilite per i documenti informatici. • Viene garantita la provenienza e la conformità con l'originale della copia cartacea di documenti informatici grazie all'apposizione a stampa di un timbro elettronico (glifo) che consente la verifica automatica della conformità, nel rispetto delle regole tecniche.

|2.2| Protocollo e fascicolo informatico

Il protocollo informatico non è materia trattata direttamente dal Codice, in quanto già ampliamente disciplinata dai precedenti provvedimenti (a partire dal Testo Unico della documentazione amministrativa n. 445/2000, in cui il legislatore ha definito 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*", ossia tutte le risorse tecnologiche necessarie alla realizzazione di un sistema automatico per la gestione elettronica dei flussi documentali).

Il nuovo Codice detta però alcune prescrizioni che ne disciplinano l'uso.

In generale, il protocollo informatico costituisce un prerequisito e una infrastruttura necessaria perché le norme del Codice possano espletare i propri effetti in termini di efficienza ed efficacia dell'azione pubblica. È utile ricordare che, in base alle norme susseguitesi dal 2000 in poi, tutte le amministrazioni sono in questo campo tenute a:

- strutturare gli Uffici di Protocollo, prevedendo le cosiddette Aree Organizzative Omogenee;
- adottare standard di protocollo e fascicoli informatici di documenti;
- creare i servizi per la tenuta del protocollo informatico e la gestione degli archivi e nominarne dei responsabili.

L'art. 40-bis del Codice, facendo esplicito riferimento al Testo Unico citato, prevede che ogni comunicazione che arrivi alla pubblica amministrazione mediante posta PEC sia comunque oggetto di registrazione di protocollo elettronico informatico.

Sempre relativamente alla formazione della documentazione amministrativa, il Codice definisce ulteriormente l'obbligo delle amministrazioni titolari di un procedimento di raccogliere in un "fascicolo informatico" gli atti, i documenti e i dati di un procedimento amministrativo da chiunque essi siano stati formati (art. 41).

Si ricorda che il fascicolo informatico deve recare l'indicazione (art. 41, comma 2-*ter*):

- dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- delle altre amministrazioni partecipanti;
- del responsabile del procedimento;
- dell'oggetto del procedimento;
- dell'elenco dei documenti contenuti.

Il Codice aggiunge ora a queste indicazioni la prescrizione di dotare i fascicoli di un apposito identificativo che ne favorisca la tracciabilità, anche in relazione all'obbligo, esplicitamente sancito dall'art. 41, di dar conto ai cittadini dello stato delle pratiche che li riguardano (cfr. Capitolo 1).

Rimane salva la possibilità di riservare l'accesso a parti del fascicolo all'amministrazione titolare o a soggetti da essa individuati[14].

Il nuovo Codice imprime dunque una forte accelerazione al processo di automazione del procedimento amministrativo e all'utilizzo del fascicolo elettronico grazie al supporto delle nuove tecnologie. Nello Schema 10 si riportano sinteticamente gli adempimenti previsti dal Codice in capo alle amministrazioni per l'implementazione del fascicolo informatico, con riferimento ai contenuti e alle caratteristiche funzionali.

[14] Fa eccezione quanto disposto dal comma 2-quater secondo cui "il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata Legge n. 241 del 1990".

Schema 10 - Il fascicolo informatico	
La PA titolare del procedimento	• Raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento da chiunque formati. • Pubblica il registro dei processi automatizzati rivolti all'utenza. • Pubblica nei propri siti un indirizzo PEC a cui il cittadino può presentare le sue richieste.
Ai fini della Pubblicità, il fascicolo informatico	• Deve poter essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento. • Deve essere affiancato da appositi strumenti per la verifica a distanza da parte del cittadino dell'avanzamento delle pratiche che lo riguardano.
Contenuto del fascicolo informatico	• Indicazione dell'amministrazione titolare del procedimento e delle altre amministrazioni partecipanti. • Individuazione del responsabile del procedimento. • Indicazione dell'oggetto del procedimento. • Elencazione dei documenti contenuti. • Indicazione dell'identificativo del fascicolo medesimo.

|2.3| Archiviazione e conservazione dei documenti digitali

Dal diritto di un cittadino o di un'impresa indicato nel nuovo Codice di inviare a una PA un documento digitale – riconosciuto valido a certe condizioni – discende una grande opportunità per le PA: dematerializzare i propri archivi e conservare i documenti in formato digitale, con grandi risparmi in termini di spazio e di tempo per la ricerca dei materiali.

Ovviamente non tutti i documenti possono essere archiviati "solo" in digitale: rimarrà una parte che dovrà essere prodotta e conservata in forma cartacea, per il particolare valore di testimonianza storica e archivistica che potrà assumere (art. 40, comma 3). Si tratta di un ristretto numero di documenti fissato per regolamento: per tutti gli altri la strada maestra è la digitalizzazione, che porterà a cambiare completamente il volto degli archivi, permettendone una dislocazione più economica ed efficiente[15].

[15] Già il Codice del 2005 permetteva in linea di principio questo processo e garantiva la validità e la rilevanza a tutti gli effetti di legge dei documenti conservati su supporti informatici, ma come vedremo le novità del nuovo CAD rendono tale principio più facilmente applicabile in concreto.

La materia della conservazione è trattata negli articoli 43, 44 e nel nuovo 44-bis del CAD. Nell'art. 43 la Legge ribadisce che "*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 e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo*"[16].

Come indicato all'art. 44, il sistema di conservazione dei documenti informatici deve assicurare il rispetto di alcuni requisiti (Schema 11):

- l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'Area Organizzativa Omogenea di riferimento;
- l'integrità del documento;
- la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari (i cosiddetti metadati);
- il rispetto delle misure di sicurezza degli archivi.

Schema 11 - La riproduzione e la conservazione dei documenti: nuovi principi e strumenti

Riproduzione e conservazione di documenti, scritture contabili, corrispondenza ecc.	• I dati riprodotti e conservati sono validi e rilevanti a tutti gli effetti di legge se la conservazione e riproduzione viene attuata con le modalità previste dalle regole tecniche. Attualmente, fino all'adozione della nuova regolamentazione, resta in vigore quanto stabilito dalla deliberazione CNIPA (ora DigitPA) n. 11/2004.
Requisiti per la conservazione	• Identificazione certa dell'autore e dell'amministrazione che ha formato il documento. • Integrità del documento. • Leggibilità e facile reperibilità dei documenti e delle informazioni identificative. • Rispetto delle misure di sicurezza.
Responsabile della conservazione	• Gestisce il sistema di conservazione in accordo con il responsabile del trattamento dei dati personali e, ove previsto, il responsabile del protocollo informatico. • Può avvalersi di soggetti (pubblici o privati) con idonee garanzie, anche esterni all'amministrazione, per la conservazione dei documenti informatici e la certificazione dei processi di conservazione.

[16] La riproduzione e la conservazione dovrà avvenire secondo le regole tecniche che dovranno essere prodotte entro 12 mesi, dopo un'approfondita consultazione con tutte le parti interessate. Nell'art. 43, comma 4 viene ribadito il potere di controllo del Ministero per i beni e le attività culturali sugli archivi di notevole interesse storico.

Le novità principali rispetto al Codice del 2005 riguardano la responsabilità della conservazione e il processo di digitalizzazione. Le nuove regole introducono strumenti più efficaci per tradurre in realtà quelle possibilità che, seppure presenti, hanno dato luogo solo ad alcune sperimentazioni. In particolare, viene introdotta la figura del "responsabile della conservazione" che:

a) deve operare d'intesa con il responsabile del trattamento dei dati personali e, dove previsto, con il responsabile del protocollo, dei flussi documentali e degli archivi (comma 1-bis), costituendo una vera e propria "*task force*";
b) può chiedere – ed è questa la principale novità – la conservazione *tout court* o la certificazione di conformità del processo di conservazione ad altri soggetti pubblici o privati che offrano adeguate garanzie sia organizzative che tecnologiche (comma 1-ter).

Due sono gli elementi innovativi introdotti dal nuovo CAD: la possibilità di avvalersi di soggetti esterni sia per la conservazione dei documenti informatici che per certificare la conformità dei processi di conservazione rispetto alle regole tecniche.

Il nuovo Codice, inoltre, apre spazio ai privati, introducendo la figura dei "conservatori accreditati" (art. 44-*bis*) e dettandone le regole, analoghe a quelle relative ai certificatori di firma digitale. In sostanza, per richiedere l'accreditamento a DigitPA (ente responsabile), i soggetti pubblici e privati hanno l'obbligo di garantire requisiti di onorabilità, di affidabilità organizzativa, tecnica e finanziaria, di competenza e di sicurezza. DigitPA, oltre alla funzione di ente accreditante, svolge compiti di vigilanza e controllo sui conservatori accreditati. Di seguito, sono sintetizzati i requisiti necessari per l'accreditamento presso DigitPA dei conservatori privati (Schema 12).

Schema 12 - Conservatori privati: i requisiti per l'accreditamento

Requisiti di amministratori e legali rappresentanti	• Stessi requisiti di onorabilità richiesti per coloro che svolgono funzioni di amministrazione, direzione e controllo presso le banche.
Requisiti dell'organizzazione	• Affidabilità organizzativa, tecnica e finanziaria. • Personale qualificato, dotato di conoscenza specifica nel settore della tecnologia delle firme elettroniche e delle procedure di sicurezza. • Utilizzo di sistemi affidabili e prodotti di firma protetti.
Forma giuridica	• Società di capitali con capitale sociale non inferiore a 200.000 euro.

In estrema sintesi, quindi, la dematerializzazione degli archivi è resa più agevole dall'introduzione di una figura responsabile e dalla possibilità di rivolgersi al mercato sia per la conservazione propriamente detta sia per certificare un processo e avere garanzia di operare in conformità con la legge.

La digitalizzazione degli archivi cartacei rende possibile un uso più razionale delle risorse potenzialmente in grado di generare risparmi, anche considerevoli. Come esplicitamente indicato dall'art.15 comma 2-*ter* del Codice, tali risparmi potranno essere utilizzati sia per incentivare il personale pubblico coinvolto nei progetti di innovazione che per finanziare nuovi progetti.

È da notare, infine, che le regole per la formazione e la conservazione digitale dei documenti, così come le regole per la loro trasmissione, si applicano anche ai privati, come stabilito dal Testo Unico della documentazione amministrativa del 2000 (DPR 445/00).

|2.4| Dati pubblici

Le prime sezioni del quinto Capo del Codice sono interamente dedicate ai dati delle pubbliche amministrazioni. In esse sono richiamati alcuni principi fondamentali, già in buona parte sanciti dal Codice del 2005:

- l'art. 50 (invariato nel nuovo Codice) stabilisce che 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 da parte delle altre pubbliche amministrazioni e dai privati;
- l'art. 51 impone l'obbligo alle amministrazioni di aggiornare tempestivamente i dati dei propri archivi non appena vengano a conoscenza dell'inesattezza degli stessi (comma 2-*bis*).

Del tutto nuova è invece la disposizione che si occupa della valorizzazione e della fruizione dei dati pubblici, sollecitando le amministrazioni a promuovere progetti di elaborazione dei dati e di diffusione degli stessi anche attraverso l'uso di strumenti di finanza di progetto (art. 52). La norma è di grande rilevanza perché sottolinea implicitamente il significativo valore economico dei dati pubblici e la necessità di aprire tale patrimonio al mercato, sia pure in forma regolata. Insieme a questa raccomandazione è previsto l'obbligo di consentire la fruizione gratuita dei dati pubblicati sui siti pubblici e l'obbligo per le amministrazioni di pubblicare dati e documenti in formato aperto. È lo stesso Codice a specificare che "*per formato dei dati di tipo aperto si intende un formato dati reso pubblico e documentato esaustivamente*" (art. 68, comma 3); al contempo è indicata la necessità di adottare soluzioni che assicurino l'interoperabilità e la cooperazione applicativa e consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto (art. 68, comma 2).

Sempre in materia di dati pubblici, il Codice prevede un'importante novità che riguarda l'accesso alle Banche dati pubbliche da parte delle PA (art. 58): il nuovo CAD impone alle amministrazioni titolari di banche dati accessibili per via telematica di predisporre, sulla base di linee guida che dovranno essere emanate entro tre mesi da DigitPA (sentito il Garante per la protezione dei dati personali), convenzioni aperte a tutte le amministrazioni per permettere l'accesso ai propri dati senza oneri[17]. La legge stabilisce che DigitPA controlli l'attuazione di questo articolo, prevedendo inoltre - in caso di mancata attuazione da parte delle PA titolari di banche dati - la nomina di un commissario *ad acta*.

Un ultimo aspetto disciplinato dal Codice, relativamente ai dati pubblici, è quello concernente le basi di dati di interesse nazionale, definite come *"l'insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni, omogenee per tipologia e contenuto, e la cui conoscenza è utilizzabile dalle PA, anche per fini statistici, per l'esercizio delle proprie funzioni e nel rispetto delle competenze e delle normative vigenti"* (art. 60, comma 1). Ogni base di dati deve essere considerata come un sistema informativo unitario che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate (art. 60, comma 2). Alcune basi di dati di interesse nazionale sono già elencate nel Codice (art. 60, comma 3-*bis*), mentre altre potranno essere successivamente introdotte entro 12 mesi per decreto (art. 60, comma 3). Tra le novità più rilevanti, il nuovo CAD descrive la "Banca dati nazionale dei contratti pubblici" che dovrà raccogliere tutte le informazioni rilevanti su tutti gli acquisti e gli appalti delle amministrazioni, sia al fine di ridurre e razionalizzare la spesa pubblica sia per un ulteriore controllo di legalità e di corretto agire, anche come prevenzione e contrasto dei fenomeni di corruzione (art. 60, commi 3 e 3-*bis*).

|2.5| Sicurezza, continuità operativa e *disaster recovery*

Il Codice prevede importanti e innovative disposizioni in merito alla sicurezza dei dati e dei sistemi, alla continuità operativa, al *disaster recovery*. Prima di riportare le principali norme dettate dal Codice è utile richiamare i concetti di continuità operativa e di *disaster recovery*.

La continuità operativa riguarda l'insieme dei metodi e degli strumenti finalizzati ad assicurare la continuità dei servizi istituzionali, anche in presenza di eventi indesiderati, che possono causare un'interruzione prolungata dei sistemi informatici. Le soluzioni per garantire la continuità dei servizi si riferiscono a tutte le componenti del "ci-

[17] L'art. 58 comma 2 del CAD stabilisce che le convenzioni (da predisporre entro 12 mesi dall'entrata in vigore del nuovo CAD) valgono anche quale autorizzazione ai sensi dell'articolo 43 comma 2 del decreto del Presidente della Repubblica n. 445 del 2000 in base al quale, per l'accesso diretto ai propri archivi, l'amministrazione certificante rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente.

clo del servizio" (tecnologia, risorse umane, ecc..). La continuità operativa considera i mezzi tecnici impiegati nei procedimenti amministrativi come strumenti per l'erogazione dei servizi ed estende la sua sfera di interesse alle tematiche più generali di natura organizzativa.

Per *disaster recovery* si intende l'insieme di misure tecnologiche atte a ripristinare i sistemi, i dati e le infrastrutture necessarie all'erogazione di servizi a fronte di gravi emergenze.

Il Codice, all'art. 50-bis, è a tal riguardo chiaro e preciso:

Comma 1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

Comma 2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

Comma 3. A tali fini, le pubbliche amministrazioni definiscono[18]*:*

a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

Comma 4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.

[18] Le pubbliche amministrazioni provvedono a definire i piani di cui all'art. 50-bis entro 15 mesi dall'entrata in vigore del nuovo CAD.

L'art. 51 al comma 1 annuncia successive regole tecniche per la sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni definendo inoltre i compiti, anche ispettivi, di DigitPA in tema di sicurezza (comma 1-*bis*).

È obbligo di ciascuna amministrazione far sì che i documenti informatici siano custoditi e controllati in modo da ridurre al minimo i rischi di distruzione, perdita o accesso non autorizzato o non consentito o non conforme (art. 51, comma 2).

Il sistema della sicurezza dei dati prevede la partecipazione di diversi soggetti istituzionali, ciascuno con compiti specifici all'interno del disegno complessivo, sintetizzati nello Schema 13.

Schema 13 - Il sistema della sicurezza dei dati: le competenze dei soggetti coinvolti

Livello istituzionale	Competenze
Presidenza del Consiglio dei Ministri o ministro per la Pubblica Amministrazione e l'Innovazione	• Emana i decreti contenenti le regole tecniche per assicurare l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.
DigitPA	• Raccorda le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici. • Promuove intese con le analoghe strutture internazionali. • Segnala al ministro per la Pubblica Amministrazione e l'Innovazione il mancato rispetto delle regole tecniche da parte delle pubbliche amministrazioni.
Pubbliche amministrazioni	• Custodiscono e controllano i documenti informatici in modo tale da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta. • Aggiornano tempestivamente i dati nei propri archivi.

|3| MODALITÀ DI COMUNICAZIONE E DI INTERAZIONE DELLA PA DIGITALE

La riforma del CAD impone alla PA di adottare soluzioni organizzative che consentano di potenziare gli strumenti e i canali per la comunicazione – a partire dal sito web – e l'interazione sia tra amministrazioni, sia tra queste e gli operatori del sistema.

|3.1| Il Sistema Pubblico di Connettività

Il Sistema Pubblico di Connettività (SPC) è la rete che collega le amministrazioni pubbliche per garantire l'interazione della PA centrale e locale con tutti gli altri soggetti connessi a internet promuovendo l'erogazione di servizi di qualità per cittadini e imprese. Il SPC è costituito dall'insieme di infrastrutture tecnologiche e di regole tecniche per lo sviluppo, la condivisione, l'integrazione e la diffusione dei dati della pubblica amministrazione.

Questa infrastruttura consente alle amministrazioni di condividere e scambiare dati e risorse informative attraverso l'interoperabilità di base ed evoluta e la cosiddetta "cooperazione applicativa" dei sistemi informatici e dei flussi informativi (vedi paragrafo successivo) secondo standard di qualità che salvaguardino la sicurezza dei dati e la riservatezza delle informazioni nel rispetto dell'autonomia del patrimonio informativo delle singole amministrazioni.

Il SPC offre alle amministrazioni interconnesse servizi di connettività, trasporto dati, interoperabilità e cooperazione applicativa secondo un modello multifornitore di acquisizione dei servizi realizzato attraverso un sistema di accordi quadro, stipulati da DigitiPA e messi a disposizione delle amministrazioni aderenti.

Grazie al nuovo Codice possono aderire al SPC anche i gestori di servizi pubblici e i soggetti che perseguono finalità di pubblico interesse, aprendo la intranet della PA agli operatori del mercato che potranno, in questo modo, scambiare dati ed informazioni in maniera sicura con l'amministrazione pubblica ed erogare servizi in cooperazione applicativa. Questo punto appare di particolare rilievo dal momento che lo scambio di dati ed informazioni fra i sistemi informativi delle amministrazioni aderenti al SPC (realizzato attraverso la cooperazione applicativa e nel rispetto delle procedure e regole tecniche di sicurezza) costituisce invio documentale valido ad ogni effetto di legge.

|3.2| Le comunicazioni tra le pubbliche amministrazioni

Un aspetto importante legato alle comunicazioni tra le pubbliche amministrazioni è rappresentato dallo scambio di documenti (art. 47).

Il Codice individua le modalità: le comunicazioni dei documenti tra le pubbliche am-

ministrazioni devono avvenire mediante l'utilizzo della posta elettronica o attraverso l'interscambio automatico di informazioni con altri sistemi -la "cooperazione applicativa"- che contempla la possibilità per un'applicazione di utilizzare in modo automatico un'informazione elaborata da un'altra applicazione (per esempio, un applicativo utilizzato all'interno di una università che preleva i dati anagrafici direttamente dal programma del Comune di residenza dello studente).

Il presupposto necessario è l'interoperabilità dei sistemi adottati dalle singole PA. Il nuovo Codice (art. 14) definisce i principi per l'implementazione, da parte delle pubbliche amministrazioni, di sistemi informativi coordinati ed interoperabili attraverso forme di collaborazione tra i diversi livelli di governo per l'individuazione di criteri condivisi.

Inoltre, qualsiasi dato trattato da una pubblica amministrazione - salvo quelli espressamente esclusi dalla legge - deve poter essere accessibile e fruibile alle altre PA (nel rispetto della normativa in materia di protezione dei dati personali) in tutti i casi in cui l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente.

Lo scambio di documenti tra le PA, attraverso posta elettronica o tramite la cooperazione applicativa, è considerato valido ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza (art. 47, comma 1). Il Codice fornisce anche i criteri in base ai quali deve essere verificata la provenienza delle comunicazioni. Queste sono valide se ricorre una delle seguenti condizioni (art. 47, comma 2):

- le comunicazioni sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
- le comunicazioni sono dotate di segnatura di protocollo conforme alla normativa vigente;
- è possibile accertarne la provenienza sulla base di quanto previsto dalla normativa vigente o dalle regole tecniche;
- le comunicazioni sono trasmesse attraverso sistemi di posta elettronica certificata.

|3.3| Siti web pubblici e trasparenza della Pubblica Amministrazione

La trasparenza dell'amministrazione pubblica è un principio cardine sia del Codice, sia della cosiddetta "riforma Brunetta", entrata in vigore con il Decreto legislativo n. 150/2009.

La riforma si riferisce alla trasparenza in termini di accessibilità totale alle informazioni concernenti ogni aspetto dell'organizzazione. L'accessibilità totale presuppone la possibilità da parte di ogni soggetto di accedere a tutte le informazioni pubbliche secondo il paradigma della "libertà di informazione" e dell'*open government* di origine statunitense.

In questo quadro, il sito istituzionale pubblico di ogni PA diventa il principale strumento di trasparenza.

L'art. 4 della Direttiva n. 8 del Ministro per la pubblica amministrazione e l'innovazione del 26 novembre 2009 prevedeva la predisposizione di Linee guida (emanate a luglio 2010) atte a suggerire alle pubbliche amministrazioni criteri e strumenti per la riduzione dei siti web pubblici obsoleti e il miglioramento di quelli attivi in termini di principi generali, gestione e aggiornamento, contenuti minimi.

La successiva Delibera n. 105/2010 della Commissione Indipendente per la Valutazione, Integrità e Trasparenza della PA (CiVIT) elenca con precisione, richiamando le suddette Linee guida per i siti web della PA, i dati e le notizie che ciascuna amministrazione deve inserire nel sito Internet.

Il Codice completa il quadro indicando come obbligatorie alcune caratteristiche fondamentali quali accessibilità, usabilità e reperibilità - anche da parte di soggetti diversamente abili - con informazioni complete, chiare, affidabili e di semplice consultazione. Esso richiama inoltre l'obbligo di tenere aggiornati i dati e di trasmetterli al Dipartimento della funzione pubblica che potrà così disporre di informazioni in tempo reale circa la consistenza dei dati esposti e dei servizi online presenti. La mancata comunicazione o aggiornamento dei dati è rilevante ai fini della valutazione della *performance* dei dirigenti.

Gli articoli 53 e 54 del Codice definiscono caratteristiche e contenuti dei siti, illustrati sinteticamente nello Schema 14.

Schema 14 - Il CAD e i contenuti dei siti web delle PA

Organizzazione, responsabilità e norme di riferimento	• L'organigramma, l'articolazione degli uffici, i nomi dei dirigenti responsabili dei singoli uffici, il settore dell'ordinamento giuridico riferibile all'attività svolta, i documenti anche normativi di riferimento.
Servizi in rete, procedimenti, avvisi e bandi	• Tipologie di procedimento svolte da ciascun ufficio di livello dirigenziale non generale, il termine per la conclusione di ciascun procedimento, il nome del responsabile e dell'unità organizzativa responsabile cui fa capo l'istruttoria, nonché dell'adozione del provvedimento finale. • Tutte le caselle di posta elettronica istituzionali attive, con particolare riferimento a quelle a cui il cittadino può inoltrare qualsiasi richiesta, assicurando un servizio che renda noti al pubblico i tempi di risposta. • I bandi di gara e di concorso. • Servizi forniti in rete già disponibili e servizi di futura attivazione, indicando i tempi previsti per l'attivazione medesima. • Il registro dei processi automatizzati rivolti al pubblico comprensivi di appositi strumenti per la verifica da parte del cittadino dell'avanzamento delle pratiche che lo riguardano.

Il nuovo Codice impone alle PA di pubblicare nei propri siti web:

- almeno un indirizzo di posta elettronica certificata a cui il cittadino può rivolgersi per qualsiasi richiesta, con l'indicazione dei tempi di risposta;
- i bandi di concorso[19].

Il Codice inoltre rammenta che la pubblicazione telematica produce effetti di pubblicità legale nei casi e nei modi espressamente previsti dall'ordinamento, e che l'amministrazione deve garantire che le informazioni contenute sui siti siano conformi e corrispondenti a quelle contenute nei provvedimenti amministrativi originali, dei quali si fornisce comunicazione tramite il sito.

Il Codice, introducendo nuovi diritti per cittadini e imprese, impone poi alle pubbliche amministrazioni di predisporre e rendere disponibile per via telematica l'elenco della documentazione richiesta per ogni procedimento assieme a moduli e formulari (art. 57, comma 1), evitando ai cittadini inutili perdite di tempo agli sportelli.

Con l'entrata in vigore del nuovo Codice, le PA devono quindi definire la documentazione richiesta per i diversi procedimenti amministrativi, i moduli e i formulari validi ad ogni effetto di legge da rendere disponibili in via telematica sui siti web pubblici. Tale obbligo si estende anche alle dichiarazioni sostitutive di certificazioni e di notorietà.

In base al Codice, le amministrazioni non possono richiedere l'uso di moduli e formulari non pubblicati sul proprio sito e, in caso di mancata pubblicazione, i relativi procedimenti possono essere avviati anche in assenza di tali moduli (art. 57, comma 2).

Ai fini delle sanzioni, l'omessa o mancata pubblicazione di moduli e formulari sono valutabili anche ai fini delle misurazioni delle *performances* individuale dei dirigenti.

|4| I SERVIZI

La portata rinnovatrice del nuovo CAD risiede, da un lato, nel compito - affidato a tutte le PA - di aumentare quantità e qualità dei beni e servizi offerti "a distanza" e, dall'altro, nel sancire un vero e proprio diritto dei cittadini-clienti di interrompere consuetudini e tradizioni nei rapporti con la PA basati su carta, code agli sportelli, moduli diversi.

Da oggi alle PA è dunque richiesto l'utilizzo di soluzioni tecnologiche e organizzative che consentano di rendere possibile l'utilizzo sicuro a servizi online di qualità attraverso innovativi strumenti di accesso e di identificazione.

La realizzazione dei servizi innovativi da parte dell'amministrazione deve dare am-

[19] A tale obbligo le PA dovranno far fronte entro il mese di luglio 2011.

pio spazio all'adozione sistematica del riuso modulare del software sviluppato dall'amministrazione stessa o da altre amministrazioni (art. 69). I programmi informatici, o parte di essi, già realizzati da un'amministrazione sono messi a disposizione delle altre amministrazioni in un'ottica di condivisione e scambio di buona prassi, prevedendo già in fase contrattuale l'inserimento di clausole che ne consentano la facile portabilità ed il riuso modulare. Per favorire la pratica del riuso, DigitPA realizza e gestisce il registro delle applicazioni tecnologiche idonee al riuso, anche in riferimento ai singoli moduli che le compongono.

|4.1| I servizi in rete, gli strumenti di accesso e di identificazione digitale

La qualità e la quantità dei servizi che le amministrazioni pubbliche mettono a disposizione dei cittadini e delle imprese sui loro siti Internet costituiscono, per molti versi, la misura della diffusione dell'e-government. I risultati sino ad ora raggiunti non sono uniformi: l'amministrazione fiscale costituisce un'eccellenza con la totale digitalizzazione dei processi (anche grazie ad un uso massiccio degli intermediari), mentre la disponibilità dei servizi in rete da parte dei Comuni e, soprattutto, il loro uso da parte dei cittadini non è ancora del tutto soddisfacente.

Il nuovo Codice interviene in questa materia, indicando, da un lato, alcuni principi generali che devono ispirare i servizi in rete e, dall'altro, puntando ad una razionalizzazione dei sistemi di accesso e di identificazione, nonché un uso più ampio e agevole dei pagamenti elettronici. Correlata a questa materia è la riorganizzazione del sistema delle firme elettroniche che garantiscono l'identificazione del soggetto e la sottoscrizione telematica dei documenti.

Tre sono i principi che l'art. 63 detta per i servizi in rete:

1. l'attenzione all'utenza, che si realizza attraverso una progettazione dei servizi che tenga sempre conto dei principi di uguaglianza, non discriminazione e di inclusività, che abbia sempre presente la possibilità di uso da parte delle fasce deboli della popolazione e che si basi su criteri di efficacia ed effettiva utilità;
2. la rilevazione del grado di soddisfazione dell'utente mediante l'adozione di strumenti immediati di feedback continui e sicuri; le amministrazioni sono inoltre tenute a garantire la completezza del procedimento in rete e la certificazione dell'esito;
3. la cooperazione tra PA, in modo da non costringere i cittadini a consultare più siti web nel caso in cui il servizio richiesto coinvolga più amministrazioni.

Come richiamato nel Capitolo 1, l'art. 64 stabilisce la possibilità per le amministrazioni di consentire l'accesso di cittadini e imprese ai servizi online non solo mediante la Carta di Identità Elettronica (CIE) e alla Carta Nazionale dei Servizi (CNS), ma anche con strumenti diversi di identificazione certa del soggetto richiedente.

In tal senso, l'art. 65 introduce la PEC quale ulteriore mezzo di identificazione per presentare istanze e dichiarazioni, come rilevato nel Capitolo 1.

|4.2| La PEC

Entro tre mesi dall'entrata in vigore del nuovo Codice si dovranno applicare le norme relative alla PEC con particolare riferimento al suo utilizzo, da parte delle PA, per tutte le comunicazioni che richiedono una ricevuta di consegna ai soggetti che hanno dichiarato preventivamente il proprio indirizzo PEC (art. 48).

Le pubbliche amministrazioni sono tenute ad inserire ed aggiornare con cadenza almeno semestrale, nell'Indice degli indirizzi delle Pubbliche Amministrazioni (IPA), i dati relativi agli indirizzi di posta elettronica e posta elettronica certificata da utilizzare per le comunicazioni, per lo scambio di informazioni e per l'invio di documenti fra le amministrazioni e fra le amministrazioni ed i cittadini[20]. In IPA devono inoltre essere indicati la struttura organizzativa dell'amministrazione, l'elenco dei servizi offerti e le informazioni relative al loro utilizzo.

L'Indice, realizzato e gestito da DigitPA, è consultabile all'indirizzo www.indicepa.gov.it.

Entro lo stesso termine verranno emanate le regole tecniche, rivolte alle amministrazioni pubbliche, per la consultazione e l'estrazione degli indirizzi PEC di professionisti e imprese, nonché di quelli dei cittadini che hanno attivato una PEC attraverso il servizio postacertificat@ (art. 6, comma 1-bis).

Schema 15 - La PEC: obblighi e opportunità per la pubblica amministrazione

La PEC per la PA	
Obblighi	• Istituire almeno un indirizzo PEC per ogni registro di protocollo. • Pubblicare gli indirizzi PEC attivi sul sito istituzionale. • Pubblicare gli indirizzi PEC sull'Indice delle Pubbliche Amministrazioni (IPA).
Opportunità	• Utilizzare la PEC per le comunicazioni telematiche che necessitano di una ricevuta di invio e di consegna. • Adottare la PEC per le comunicazioni con i cittadini, professionisti, imprese e altre pubbliche amministrazioni. • Disporre degli elenchi di indirizzi PEC relativi a imprese, professionisti e cittadini che preventivamente hanno dichiarato il proprio indirizzo.

[20] Vedi artt. 47 e 57-bis

|4.3| Pagamenti elettronici

Con la finalità di rendere i pagamenti a favore delle amministrazioni più semplici, veloci e tracciabili, il nuovo Codice dell'Amministrazione Digitale ha introdotto il principio dei pagamenti alle amministrazioni pubbliche per mezzo di alcune tipologie di tecnologie digitali.

Nella prima edizione del Codice 2005 esisteva già questa possibilità, ma non era identificata espressamente la modalità con la quale effettuare le transazioni.

L'art. 5 del nuovo Codice richiama il principio secondo il quale le amministrazioni devono consentire l'effettuazione dei pagamenti con modalità informatiche su tutto il territorio nazionale, fatte salve le "*attività di riscossione dei tributi regolate da norme specifiche*".

Gli strumenti operativi (come le carte di credito, di debito o prepagate, ovvero: gli strumenti di pagamento elettronico con effetto equivalente) vengono espressamente indicati per le amministrazioni centrali, lasciando libertà di adeguamento alle Regioni e ai propri enti, nonché alle amministrazioni del Servizio Sanitario Nazionale e agli enti locali.

Lo stesso articolo detta anche le modalità con cui garantire ai privati la relativa effettuazione dei pagamenti, lasciando alle amministrazioni centrali la facoltà di individuare un prestatore di servizi di pagamento per la riscossione.

Spetterà al prestatore indicato dall'amministrazione centrale, nel momento in cui riceve il pagamento dovuto, riversare le somme ricevute al tesoriere dell'ente. Tali operazioni vanno registrate in un apposito sistema informatico a disposizione dell'amministrazione indicante il pagamento eseguito e la relativa causale, la corrispondenza di ciascun pagamento, i capitoli e gli articoli d'entrata oppure le contabilità speciali interessate (comma 2).

Le operazioni di pagamento sopra descritte, i tempi di decorrenza della nuova disciplina e l'insieme dei rapporti tra amministrazione e prestatore dei servizi saranno oggetto, entro sei mesi dall'entrata in vigore del nuovo CAD, di specificazione in un decreto del ministro per la Pubblica Amministrazione e l'Innovazione e dei ministri competenti per materia, di concerto con il ministro dell'Economia e delle Finanze, sentito DigitPA (comma 3).

L'effetto di questa misura, da un lato, consentirà di mettere in condizione tutte le amministrazioni di gestire la riscossione dei pagamenti con modalità più sicure e rintracciabili e, dall'altro, permetterà a tutti gli operatori privati di eseguire facilmente le operazioni di pagamento utilizzando il canale digitale.

PARTE II

Codice dell'amministrazione digitale

Decreto legislativo 7 marzo 2005, n. 82

Il testo è stato redatto al fine di facilitare la lettura del Codice dell'Amministrazione Digitale a seguito delle modifiche ed integrazioni introdotte dal Decreto legislativo 30 dicembre 2010, n. 235, pubblicato nel Supplemento ordinario n. 8 alla Gazzetta Ufficiale n. 6 del 10 gennaio 2011 ed indicate in carattere grassetto corsivo.

Il Presidente della Repubblica

Visti gli articoli 76, 87 e 117, secondo comma, lettera r), della Costituzione;

Visto l'articolo 14 della legge 23 agosto 1988, n. 400, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri;

Visto l'articolo 10 della legge 29 luglio 2003, n. 229, recante interventi in materia di qualità della regolazione, riassetto normativo e codificazione - legge di semplificazione 2001;

Vista la legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

Visto il decreto legislativo 12 febbraio 1993, n. 39, recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'articolo 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421;

Visto il decreto legislativo 30 luglio 1999, n. 300, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri;

Visto il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Testo A), di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

Visto il decreto legislativo 30 marzo 2001, n. 165, recante norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;

Visto il decreto legislativo 23 gennaio 2002, n. 10, recante attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali;

Vista la legge 9 gennaio 2004, n. 4, recante disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici;

Visto il decreto legislativo 20 febbraio 2004, n. 52, recante attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA;

Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione dell'11 novembre 2004;

Esperita la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del 22 giugno 1998 del Parlamento europeo e del Consiglio, modificata dalla direttiva 98/48/CE del 20 luglio 1998 del Parlamento europeo e del Consiglio, attuata dalla legge 21 giugno 1986, n. 317,

così come modificata dal decreto legislativo 23 novembre 2000, n. 427;

Acquisito il parere della Conferenza unificata, ai sensi dell'articolo 8, del decreto legislativo 28 agosto 1997, n. 281, espresso nella riunione del 13 gennaio 2005;

Sentito il Garante per la protezione dei dati personali;

Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 7 febbraio 2005;

Acquisito il parere delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 4 marzo 2005;

Sulla proposta del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, con il Ministro dell'economia e delle finanze, con il Ministro dell'interno, con il Ministro della giustizia, con il Ministro delle attività produttive e con il Ministro delle comunicazioni;

Emana il seguente decreto legislativo

|CAPO I| PRINCIPI GENERALI

|SEZIONE I| DEFINIZIONI, FINALITÀ E ÀMBITO 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 del documento informatico: la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione;

   c) carta d'identità elettronica: il documento d'identità munito ***di elementi per l'identificazione fisica*** 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 all'identità del titolare i dati utilizzati per verificare le firme elettroniche;

   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;

   i-bis) copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

   i-ter) copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

   i- quater) copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informa-

tico con diversa sequenza di valori binari;

i- quinquies) duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

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;

p-bis) documento analogico: la rappresentazione non 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 identificazione informatica;

q-bis) firma elettronica avanzata: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

r) firma elettronica qualificata: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

s) firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e 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;

u-bis) gestore di posta elettronica certificata: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata;

u-ter) identificazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;

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;

v-bis) posta elettronica certificata: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai 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 àmbito 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, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, nonché alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1, comma 5, della legge 30 dicembre 2004, n. 311.

2-*bis*. Abrogato.

3. ***le disposizioni di cui al Capo II, agli articoli 40, 43 e 44 del Capo III, nonché al Capo IV, si applicano ai privati ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e successive modificazioni.***

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 del codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196. I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

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. ***Con decreti del Presidente del Consiglio dei ministri, tenuto conto delle esigenze derivanti dalla natura delle proprie particolari funzioni, sono stabiliti le modalità, i limiti ed i tempi di applicazione delle disposizioni del presente Codice alla Presidenza del Consiglio dei Ministri, nonché all'Amministrazione economico-finanziaria***

|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, ***con i soggetti di cui all'articolo 2, comma 2, e con i gestori di pubblici servizi ai sensi di quanto previsto dal presente codice.***

1-*bis*. Abrogato.

1-*ter*. La tutela giurisdizionale davanti al giudice amministrativo è disciplinata dal codice del processo amministrativo.

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. *Le pubbliche amministrazioni consentono, sul territorio nazionale, l'effettuazione dei pagamenti ad esse spettanti, a qualsiasi titolo dovuti, fatte salve le attività di riscossione dei tributi regolate da specifiche normative, con l'uso delle tecnologie dell'informazione e della comunicazione.*

2. *Le pubbliche amministrazioni centrali possono avvalersi, senza nuovi o maggiori oneri per la finanza pubblica, di prestatori di servizi di pagamento per consentire ai privati di effettuare i pagamenti in loro favore attraverso l'utilizzo di carte di debito, di credito o prepagate e di ogni altro strumento di pagamento elettronico disponibile. Il prestatore dei servizi di pagamento che riceve l'importo dell'operazione di pagamento, effettua il riversamento dell'importo trasferito al tesoriere dell'ente, registrando in apposito sistema informatico, a disposizione dell'amministrazione, il pagamento eseguito e la relativa causale, la corrispondenza di ciascun pagamento, i capitoli e gli articoli d'entrata oppure le contabilità speciali interessate.*

3. *Con decreto del Ministro per la pubblica amministrazione e l'innovazione ed i Ministri competenti per materia, di concerto con il Ministro dell'economia e delle finanze, sentito DigitPA sono individuate le operazioni di pagamento interessate dai commi 1 e 2, i tempi da cui decorre la disposizione di cui al comma 1, le relative modalità per il riversamento, la rendicontazione da parte del prestatore dei servizi di pagamento e l'interazione tra i sistemi e i soggetti coinvolti nel pagamento, nonché il modello di convenzione che il prestatore di servizi di pagamento deve sottoscrivere per effettuare il servizio.*

4. *Le regioni, anche per quanto concerne i propri enti e le amministrazioni del Servizio sanitario nazionale, e gli enti locali adeguano i propri ordinamenti al principio di cui al comma 1.*

5-bis. Comunicazioni tra imprese e amministrazioni pubbliche

1. *La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.*

2. *Con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro per la pubblica amministrazione e l'innovazione, di concerto con il Ministro dello sviluppo economico e con il Ministro per la semplificazione normativa, sono adotta-*

te le modalità di attuazione del comma 1 da parte delle pubbliche amministrazioni centrali e fissati i relativi termini.

3. DigitPA, anche avvalendosi degli Uffici di cui all'articolo 17, provvede alla verifica dell'attuazione del comma 1 secondo le modalità e i termini indicati nel decreto di cui al comma 2.

4. Il Governo promuove l'intesa con regioni ed enti locali in sede di Conferenza unificata per l'adozione degli indirizzi utili alla realizzazione delle finalità di cui al comma 1.

6. Utilizzo della posta elettronica certificata

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

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

2. Abrogato.

2-bis. Abrogato.

7. Qualità dei servizi resi e soddisfazione dell'utenza

1. Le pubbliche amministrazioni 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. ***Le pubbliche amministrazioni favoriscono*** 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. Sportello unico per le attività produttive

1. ***Lo sportello unico per le attività produttive di cui all'articolo 38, comma 3, del decreto-legge 25 giugno 2008, n.112, convertito, con modificazioni, dalla legge 6 agosto 2008, n.133, eroga i propri servizi verso l'utenza in via telematica.***

2. ***Abrogato.***

3. ***Abrogato.***

4. Lo Stato realizza, nell'àmbito di quanto previsto dal Sistema Pubblico di Connettività di cui al presente decreto, 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 del-

le 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***, nonché per la garanzia dei diritti dei cittadini e delle imprese di cui al Capo I, sezione II, del presente decreto.***

1-***bis. Gli organi di governo nell'esercizio delle funzioni di indirizzo politico ed in particolare nell'emanazione delle direttive generali per l'attività amministrativa e per la gestione ai sensi del comma 1 dell'articolo 14 del decreto legislativo 30 marzo 2001, n. 165, e le amministrazioni pubbliche nella redazione del piano di performance di cui all'articolo 10 del decreto legislativo 27 ottobre 2009, n.150, dettano disposizioni per l'attuazione delle disposizioni del presente decreto.***

1-*ter*. I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al presente decreto ai sensi e nei limiti degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165, ferme restando le eventuali responsabilità penali, civili e contabili previste dalle norme vigenti. ***L'attuazione delle disposizioni del presente decreto è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti.***

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, ***ivi comprese le reti di telefonia fissa e mobile in tutte le loro articolazioni 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.

5-*bis*. Le pubbliche amministrazioni implementano e consolidano i processi di informatizzazione in atto, ivi compresi quelli riguardanti l'erogazione ***attraverso le tecnologie dell'informazione e della comunicazione*** in via telematica di servizi a cittadini ed imprese anche con l'intervento di privati.

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.

2-bis. Le regioni promuovono sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali.

2-ter. Le regioni e gli enti locali digitalizzano la loro azione amministrativa e implementano l'utilizzo delle tecnologie dell'informazione e della comunicazione per garantire servizi migliori ai cittadini e alle imprese.

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.

3-bis. Ai fini di quanto previsto ai commi 1, 2 e 3, è istituita senza nuovi o maggiori oneri per la finanza pubblica, presso la Conferenza unificata, previa delibera della medesima che ne definisce la composizione e le specifiche competenze, una Commissione permanente per l'innovazione tecnologica nelle regioni e negli enti locali con funzioni istruttorie e consultive.

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.

2-bis. Le Pubbliche amministrazioni nella valutazione dei progetti di investimento in materia di innovazione tecnologica tengono conto degli effettivi risparmi derivanti dalla razionalizzazione di cui al comma 2, nonché dei costi e delle economie che ne derivano.

2-ter. Le Pubbliche amministrazioni, quantificano annualmente, ai sensi dell'articolo 27, del decreto legislativo 27 ottobre 2009, n.150, i risparmi effettivamente conseguiti in attuazione delle disposizioni di cui ai commi 1 e 2. Tali risparmi sono utilizzati, per due terzi secondo quanto previsto dall'articolo 27, comma 1, del citato decreto legislativo n. 150 del 2009 e in misura pari ad un terzo per il finanziamento di ulteriori progetti di innovazione.

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 inter-

vento 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 unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali Uffici, responsabile del coordinamento funzionale. Al predetto Ufficio afferiscono i compiti relativi a:
   a) coordinamento strategico dello sviluppo dei sistemi informativi ***di telecomunicazione e fonia***, 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 ***di telecomunicazione e fonia*** dell'amministrazione;
   c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al Sistema Pubblico di Connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;
   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 ***di telecomunicazione e fonia***;
   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 coopera-

zione 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 accessibilità e fruibilità.

1-bis. Per lo svolgimento dei compiti di cui al comma 1, le Agenzie, le Forze armate, compresa l'Arma dei carabinieri e il Corpo delle capitanerie di porto, nonché i Corpi di polizia hanno facoltà di individuare propri Uffici senza incrementare il numero complessivo di quelli già previsti nei rispettivi assetti organizzativi.

1-ter. DigitPA assicura il coordinamento delle iniziative di cui al comma 1, lettera c), con le modalità di cui all'articolo 51.

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 [oggi DigitPA], 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 ***memorizzazione*** su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

2. Abrogato.

3. ***Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, 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.

5-bis. 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.

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, sicurezza, integrità e immodificabilità.

2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che ga-

rantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.

2-bis). Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale.

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. Copie informatiche di documenti analogici

1. ***I documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, 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. La loro esibizione e produzione sostituisce quella dell'originale.***

2. ***Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata 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.***

3. *Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.*

4. *Le copie formate ai sensi dei commi 1, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.*

5. *Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.*

6. *Fino alla data di emanazione del decreto di cui al comma 5r per tutti i documenti analogici originali unici permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.*

23. Copie analogiche di documenti informatici

1. *Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.*

2. *Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.*

23-bis. Duplicati e copie informatiche di documenti informatici

1. *I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche di cui all'articolo 71.*

2. *Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti*

le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

23-ter. Documenti amministrativi informatici

1. *Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.*

2. *I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile.*

3. *Le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli 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 o di altra firma elettronica qualificata e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico.*

4. *Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, 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 sentiti DigitPA e il Garante per la protezione dei dati personali.*

5. *Al fine di assicurare la provenienza e la conformità all'originale, sulle copie analogiche di documenti informatici, è apposto a stampa, sulla base dei criteri definiti con linee guida emanate da DigitPA, un contrassegno generato elettronicamente, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 e tale da consentire la verifica automatica della conformità del documento analogico a quello informatico.*

6. *Per quanto non previsto dal presente articolo si applicano gli articoli 21, 22 , 23 e 23-bis.*

23-quater. Riproduzioni informatiche

1. *All'articolo 2712 del codice civile dopo le parole: «riproduzioni fotografiche» è inserita la seguente: «informatiche».*

|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 elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.***

2. ***L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata 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 dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.***

3. ***L'apposizione della firma digitale 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, ***qualora emettano certificati qualificati,*** devono possedere i requisiti di onorabilità richiesti ai sogget-

ti 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;
   d) 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 [oggi DigitPA], attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice.

4. Il CNIPA [oggi DigitPA] 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 del certificatore che ha rilasciato il certificato, realizzata in conformità alle regole tecniche ed idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo.

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 contenere, 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, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;
   b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera *a*) 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.

3-bis. Le informazioni di cui al comma 3 possono essere contenute in un separato certificato elettronico e possono essere rese disponibili anche in rete. Con decreto del Presidente del Consiglio dei Ministri sono definite le modalità di attuazione del presente comma, anche in riferimento alle pubbliche amministrazioni e agli ordini professionali.

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 li-

vello più elevato, in termini di qualità e di sicurezza, chiedono di essere accreditati presso il CNIPA [oggi DigitPA].

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 [oggi DigitPA] 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 [oggi DigitPA] dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal CNIPA [oggi DigitPA] 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. Il valore giuridico delle firme elettroniche qualificate e delle firme digitali basate su certificati qualificati rilasciati da certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE è equiparato a quello previsto per le firme elettroniche qualificate e per le firme digitali basate su certificati qualificati emessi dai certificatori accreditati ai sensi del presente articolo.

9. Alle attività previste dal presente articolo si fa fronte nell'àmbito delle risorse del CNIPA [oggi DigitPA], 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 certificato 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 dei certificatori e dei gestori di posta elettronica certificata

1. ***DigitPA svolge funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e dei gestori di posta elettronica certificata.***

32. Obblighi del titolare e del certificatore

1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di forma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.

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) (soppressa);
   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 venti 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.

m-bis) garantire il corretto funzionamento e la continuità del sistema e comunicare immediatamente a DigitPA e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso.

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

32 –bis. Sanzioni per i certificatori qualificati e per i gestori di posta elettronica certificata

1. ***Qualora si verifichi, salvi i casi di forza maggiore o caso fortuito, un malfunzionamento nel sistema che determini un disservizio, ovvero la mancata o intempestiva comunicazione dello stesso disservizio a DigitPA o agli utenti, ai sensi dell'articolo 32, comma 3, lettera m-bis), DigitPA diffida il certificatore qualificato o il gestore di posta elettronica certificata a ripristinare la regolarità del servizio o ad effettuare le comunicazioni ivi previste. Se il disservizio ovvero la mancata o intempestiva comunicazione sono reiterati per due volte nel corso di un biennio, successivamente alla seconda diffida si applica la sanzione della cancellazione dall'elenco pubblico.***

2. ***Qualora si verifichi, fatti salvi i casi di forza maggiore o di caso fortuito, un malfunzionamento nel sistema che determini l'interruzione del servizio, ovvero la mancata o intempestiva comunicazione dello stesso disservizio a DigitPA o agli utenti, ai sensi dell'articolo 32, comma 3, lettera m-bis), DigitPA diffida il certificatore qualificato o il gestore di posta elettronica certificata a ripristinare la regolarità del servizio o ad effettuare le comunicazioni ivi previste. Se l'interruzione del servizio ovvero la mancata o intempestiva comunicazione sono reiterati nel corso di un biennio, successivamente alla prima diffida si applica la sanzione della cancellazione dall'elenco pubblico.***
3. ***Nei casi di cui ai commi 1 e 2 può essere applicata la sanzione amministrativa accessoria della pubblicazione dei provvedimenti di diffida o di cancellazione secondo la legislazione vigente in materia di pubblicità legale.***

4. ***Qualora un certificatore qualificato o un gestore di posta elettronica certificata non ottemperi, nei tempi previsti, a quanto prescritto da DigitPA nell'esercizio delle attività di vigilanza di cui all'articolo 31 si applica la disposizione di cui al comma 2.***

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 ***venti anni decorrenti dall'emissione*** 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 ad esclusione di quelli rilasciati da collegi e ordini professionali e relativi organi agli iscritti nei rispettivi albi e registri; 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 71.

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. La firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima.

4. I dispositivi sicuri di firma devono essere dotati di certificazione di sicurezza ai sensi dello schema nazionale 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 ***dall'Organismo di certificazione della sicurezza informatica***, 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. ***L'attuazione dello schema nazionale non deve determinare nuovi o maggiori oneri per il bilancio dello Stato.*** 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 di cui al comma 5 è inoltre riconosciuta se accertata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 11, paragrafo 1, lettera b), della direttiva 1999/93/CE.

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 dell'articolo 37;
   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 [oggi DigitPA] 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 [oggi DigitPA] rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 29, comma 6.

4-bis. Qualora il certificatore qualificato cessi la propria attività senza indicare, ai sensi del comma 2, un certificatore sostitutivo e non si impegni a garantire la conservazione e la disponibilità della documentazione prevista dagli articoli 33 e 32, comma 3, lettera j) e delle ultime liste di revoca emesse, deve provvedere al deposito presso DigitPA che ne garantisce la conservazione e la disponibilità.

|SEZIONE III| TRASFERIMENTI DI FONDI, LIBRI E SCRITTURE

38. Trasferimenti di fondi

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 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. Abrogato

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.

40-bis. Protocollo informatico

1. Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica di cui agli articoli 47, commi 1 e 3, 54, comma 2-ter e 57-bis, comma 1, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle regole tecniche di cui all'articolo 71.

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.

1-bis. La gestione dei procedimenti amministrativi è attuata in modo da consentire, mediante strumenti automatici, il rispetto di quanto previsto all'articolo 54, commi 2-ter e 2-quater.

2. La pubblica amministrazione titolare del procedimento raccoglie 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 ago-

sto 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.

2-bis. Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento. Le regole per la costituzione, l'identificazione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico ed il Sistema Pubblico di Connettività, e comunque rispettano i criteri dell'interoperabilità e della cooperazione applicativa; regole tecniche specifiche possono essere dettate ai sensi dell'articolo 71, di concerto con il Ministro della funzione pubblica.

2-ter. Il fascicolo informatico reca l'indicazione:

a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
b) delle altre amministrazioni partecipanti;
c) del responsabile del procedimento;
d) dell'oggetto del procedimento;
e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater.

e-bis) dell'identificativo del fascicolo medesimo.

2-quater. Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990.

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 recu pero 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 e la conservazione nel tempo sono effettuate*** in modo da garantire la conformità dei documenti agli originali, 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***, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.***

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 ***assicura***:
   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.

1-bis. Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza.

1-ter. Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche.

44-bis. Conservatori accreditati

1. I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono l'accreditamento presso DigitPA.

2. ***Si applicano, in quanto compatibili, gli articoli 26, 27, 29, ad eccezione del comma 3, lettera a) e 31.***

3. ***I soggetti privati di cui al comma 1 sono costituiti in società di capitali con capitale sociale non inferiore a euro 200.000.***

|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, 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 mediante l'utilizzo della posta elettronica ***o in cooperazione applicativa***; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

2. Ai fini della verifica della provenienza le comunicazioni sono valide se:
   a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
   b) ovvero sono dotate di ***segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445***;
   c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71;
   d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

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

48. Posta elettronica certificata

1. ***La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA.***

2. ***La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.***

3. ***La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi al decreto del Presidente del Consiglio dei Ministri di cui al comma 1.***

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 per la prestazione di elaborazioni aggiuntive*** 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 presente decreto.

50-bis. Continuità operativa

1. ***In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.***

2. ***Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.***

3. ***A tali fini, le pubbliche amministrazioni definiscono:***
   a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche af-

fidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.

51. Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni

1. Con le regole tecniche adottate ai sensi dell'articolo 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.

1-bis. DigitPA, ai fini dell'attuazione del comma 1:

a) raccorda le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;

b) promuove intese con le analoghe strutture internazionali;

c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni".

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.

2-bis. Le amministrazioni hanno l'obbligo di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi.

52. Accesso telematico e riutilizzazione dei 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 di-

sciplinano l'esercizio del diritto di accesso sono pubblicati su siti pubblici accessibili per via telematica.

1-bis. Le pubbliche amministrazioni, al fine di valorizzare e rendere fruibili i dati pubblici di cui sono titolari, promuovono progetti di elaborazione e di diffusione degli stessi anche attraverso l'uso di strumenti di finanza di progetto, assicurando:

a) il rispetto di quanto previsto dall'articolo 54, comma 3;

b) la pubblicazione dei dati e dei documenti in formati aperti di cui all'articolo 68, commi 3 e 4.

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. Sono in particolare resi facilmente reperibili e consultabili i dati di cui all'articolo 54.

2. Il CNIPA [oggi DigitPA] 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 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, i nomi dei dirigenti responsabili dei singoli uffici, 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;

g) l'elenco dei servizi forniti in rete già disponibili e dei servizi di futura attivazione, indicando i tempi previsti per l'attivazione medesima.
g-bis) i bandi di concorso.

1-bis. Le pubbliche amministrazioni centrali comunicano in via telematica alla Presidenza del Consiglio dei Ministri – Dipartimento della funzione pubblica i dati di cui alle lettere b), c), g) e g-bis) del comma 1, secondo i criteri e le modalità di trasmissione e aggiornamento individuati con circolare del Ministro per la pubblica amministrazione e l'innovazione. I dati di cui al periodo precedente sono pubblicati sul sito istituzionale del Dipartimento della funzione pubblica. La mancata comunicazione o aggiornamento dei dati è comunque rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti.

2 Abrogato
2-bis Abrogato
2-ter. Le amministrazioni pubbliche pubblicano nei propri siti un indirizzo istituzionale di posta elettronica certificata a cui il cittadino possa rivolgersi per qualsiasi richiesta ai sensi del presente codice. Le amministrazioni devono altresì assicurare un servizio che renda noti al pubblico i tempi di risposta.

2-*quater*. Le amministrazioni pubbliche che già dispongono di propri siti devono pubblicare il registro dei processi automatizzati rivolti al pubblico. Tali processi devono essere dotati di appositi strumenti per la verifica a distanza da parte del cittadino dell'avanzamento delle pratiche ***che lo riguardano.***

3. I dati pubblici contenuti nei siti delle pubbliche amministrazioni sono fruibili in rete gratuitamente e senza necessità di ***identificazione*** 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.

4-*bis*. La pubblicazione telematica produce effetti di pubblicità legale nei casi e nei modi espressamente previsti dall'ordinamento.

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 all'autorità giudiziaria di ogni ordine e grado

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 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, osservando le cautele previste dalla normativa in materia di tutela dei dati personali.

2-bis. I dati identificativi delle questioni pendenti, le sentenze e le altre decisioni depositate in cancelleria o segreteria dell'autorità giudiziaria di ogni ordine e grado sono, comunque, rese accessibili ai sensi dell'articolo 51 del codice in materia di protezione dei dati personali approvato con decreto legislativo n. 196 del 2003.

57. Moduli e formulari

1. Le pubbliche amministrazioni provvedono a definire e a ***rendere disponibili 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. Le pubbliche amministrazioni non possono richiedere l'uso di moduli e formulari che non siano stati pubblicati; in caso di omessa pubblicazione, i relativi procedimenti possono essere avviati anche in assenza dei suddetti moduli o formulari. La mancata pubblicazione è altresì rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti responsabili..

57-bis. Indice degli indirizzi delle pubbliche amministrazioni

1. Al fine di assicurare la trasparenza delle attività istituzionali è istituito l'indice degli indirizzi delle amministrazioni pubbliche, nel quale sono indicati gli indirizzi di posta elettronica da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge fra le amministrazioni e fra le amministrazioni ed i cittadini.

2. La realizzazione e la gestione dell'indice sono affidate a DigitPA, che può utilizzare a tal fine elenchi e repertori già formati dalle amministrazioni pubbliche.

3. Le amministrazioni aggiornano gli indirizzi ed i contenuti dell'indice con cadenza almeno semestrale, salvo diversa indicazione del CNIPA [oggi DigitPA]. La mancata comunicazione degli elementi necessari al completamento dell'indice e del loro aggiornamento è valutata ai fini della responsabilità dirigenziale e dell'attribuzione della retribuzione di risultato ai dirigenti responsabili.

|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. Ai sensi dell'articolo 50, comma 2, nonché al fine di agevolare l'acquisizione d'ufficio ed il controllo sulle dichiarazioni sostitutive riguardanti informazioni e dati relativi a stati, qualità personali e fatti di cui agli articoli 46 e 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le Amministrazioni titolari di banche dati accessibili per via telematica predispongono, sulla base delle linee guida redatte da DigitPA, sentito il Garante per la protezione dei dati personali, apposite convenzioni aperte all'adesione di tutte le amministrazioni interessate volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti, senza oneri a loro carico. Le convenzioni valgono anche quale autorizzazione ai sensi dell'articolo 43, comma 2, del citato decreto del Presidente della Repubblica n. 445 del 2000.

3. DigitPA provvede al monitoraggio dell'attuazione del presente articolo, riferendo annualmente con apposita relazione al Ministro per la pubblica amministrazione e l'innovazione e alla Commissione per la valutazione, la trasparenza e l'integrità delle amministrazione pubbliche di cui all'articolo 13 del decreto legislativo 27 ottobre 2009, n. 150.

3-bis. In caso di mancata predisposizione delle convenzioni di cui al comma 2, il Presidente del Consiglio dei Ministri stabilisce un termine entro il quale le amministrazioni interessate devono provvedere. Decorso inutilmente il termine, il Presidente del Consiglio dei Ministri può nominare un commissario ad acta incaricato di predisporre le predette convenzioni. Al Commissario non spettano compensi, indennità o rimborsi.

3-ter. Resta ferma la speciale disciplina dettata in materia di dati territoriali.

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 presente decreto che disciplinano il Sistema Pubblico di Connettività.

3. Per agevolare la pubblicità dei dati di interesse generale, disponibili presso le pubbliche amministrazioni a livello nazionale, regionale e locale, presso il CNIPA [oggi DigitPA] 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. ***Con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione,*** di concerto con il Ministro dell'ambiente e della tutela del territorio e del mare, per i profili relativi ai dati ambientali, 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.

7-bis. Nell'ambito dei dati territoriali di interesse nazionale rientra la base dei dati catastali gestita dall'Agenzia del territorio. Per garantire la circolazione e la fruizione dei dati catastali conformemente alle finalità ed alle condizioni stabilite dall'articolo 50, il direttore dell'Agenzia del territorio, di concerto con il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni e previa intesa con la Conferenza unificata, definisce con proprio decreto entro la data del 30 giugno 2006, in coerenza con le disposizioni che disciplinano il Sistema Pubblico di Connettività, le regole tecnico economiche per l'utilizzo dei dati catastali per via telematica da parte dei sistemi informatici di altre amministrazioni.

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***, anche per fini statistici,*** 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 73 e secondo le vigenti regole del Sistema statistico nazionale di cui al decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni***.

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 ***sentiti il Garante per la protezione dei dati personali e l'Istituto nazionale di statistica.*** 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.

3-bis. In sede di prima applicazione e fino all'adozione del decreto di cui al comma 3, sono individuate le seguenti basi di dati di interesse nazionale:

- ***a) repertorio nazionale dei dati territoriali;***
- ***b) indice nazionale delle anagrafi;***
- ***c) banca dati nazionale dei contratti pubblici di cui all'articolo 62-bis;***
- ***d) casellario giudiziale;***
- ***e) registro delle imprese;***
- ***f) gli archivi automatizzati in materia di immigrazione e di asilo di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 27 luglio 2004, n. 242.***

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 e nel rispetto delle regole tecniche concernenti il Sistema Pubblico di Connettività, in coerenza con le quali il Ministero dell'interno definisce le regole di sicurezza per l'accesso e per la gestione delle informazioni anagrafiche e fornisce i servizi di convalida delle informazioni medesime ove richiesto per l'attuazione della normativa vigente.

62-bis. Banca dati nazionale dei contratti pubblici

1. **Per favorire la riduzione degli oneri amministrativi derivanti dagli obblighi informativi ed assicurare l'efficacia, la trasparenza e il controllo in tempo reale dell'azione amministrativa per l'allocazione della spesa pubblica in lavori, servizi e forniture, anche al fine del rispetto della legalità e del corretto agire della pubblica amministrazione e prevenire fenomeni di corruzione, si utilizza la "Banca dati nazionale dei contratti pubblici" (BDNCP) istituita, presso l'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture, della quale fanno parte i dati previsti dall'articolo 7 del decreto legislativo 12 aprile 2006, n. 163, e disciplinata, ai sensi del medesimo decreto legislativo, dal relativo regolamento attuativo.**

|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 e i gestori di servizi pubblici 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, A tal fine, sono tenuti ad adottare strumenti idonei alla rilevazione immediata, continua e sicura del giudizio degli utenti, in conformità alle regole tecniche da emanare ai sensi dell'articolo 71. Per le amministrazioni e i gestori di servizi pubblici regionali e locali le regole tecniche sono adottate previo parere della Commissione permanente per l'innovazione tecnologica nelle regioni e negli enti locali di cui all'articolo 14, comma 3-bis.***

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'***identificazione*** informatica.

2. ***Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio.*** 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. ***Abrogato***

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, ***nonché quando le istanze e le dichiarazioni sono inviate con le modalità di cui all'articolo 38, comma 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.***

   c-bis) ovvero se trasmesse dall'autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce dichiarazione vincolante ai sensi dell'articolo 6, comma 1, secondo periodo. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario.

1-bis. Con decreto del Ministro per la pubblica amministrazione e l'innovazione e del Ministro per la semplificazione normativa, su proposta dei Ministri competenti per materia, possono essere individuati i casi in cui è richiesta la sottoscrizione mediante firma digitale.

2. Le istanze e le dichiarazioni inviate o compilate sul sito 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. Abrogato

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 ***dell'età prevista dalla legge per il rilascio della carta d'identità elettronica***, 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 ***dell'età prevista dalla legge per il rilascio della carta d'identità elettronica***, 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 ***dell'età prevista dalla legge per il rilascio della carta d'identità elettronica***, 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.

8-bis. Fino al 31 dicembre 2011, la carta nazionale dei servizi e le altre carte elettroniche ad essa conformi possono essere rilasciate anche ai titolari di carta di identità elettronica.

|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 [oggi DigitPA]; 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***, o parti di essi,*** 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, quando possibile modulari, basate sui sistemi funzionali resi noti ai sensi dell'articolo 70, che assicurino l'interoperabilità e la cooperazione applicativa e consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto, salvo che ricorrano motivate ed eccezionali esigenze.

2-bis. Le amministrazioni pubbliche comunicano tempestivamente al DigitPA l'adozione delle applicazioni informatiche e delle pratiche tecnologiche, e organizzative,adottate, fornendo ogni utile informazione ai fini della piena conoscibilità delle soluzioni adottate e dei risultati ottenuti, anche per favorire il riuso e la più ampia diffusione delle migliori pratiche.

3. Per formato dei dati di tipo aperto si intende un formato dati reso pubblico e documentato esaustivamente.

4. Il CNIPA [oggi DigitPA] 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 ***informatici*** 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 ***e conformi alla definizione e regolamentazione effettuata da DigitPA, ai sensi dell'articolo 68, comma 2.***

3. Le pubbliche amministrazioni inseriscono, nei contratti per l'acquisizione di programmi informatici ***o di singoli moduli***, 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 dei programmi o dei singoli moduli.*** Le clausole suddette definiscono le condizioni da osservare per la prestazione dei servizi indicati.

70. Banca dati dei programmi informatici riutilizzabili

1. ***DigitPA, sentita 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 anche con riferimento a singoli moduli,segnalando quelle che, in base alla propria valutazione, si configurano quali migliori pratiche organizzative e tecnologiche.***

2. Le pubbliche amministrazioni centrali che intendono acquisire programmi applicativi valutano preventivamente la possibilità di riuso delle applicazioni analoghe rese note dal CNIPA [oggi DigitPA] 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 la pubblica amministrazione e l'innovazione, di concerto con i Ministri competenti, 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, previa acquisizione obbligatoria del parere tecnico di DigitPA.***

1-bis. Abrogato

1-ter. Le regole tecniche di cui al presente codice sono dettate in conformità alle discipline risultanti dal processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea.

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| SISTEMA PUBBLICO DI CONNETTIVITÀ E RETE INTERNAZIONALE DELLA PUBBLICA AMMINISTRAZIONE

|SEZIONE I| DEFINIZIONI RELATIVE AL SISTEMA PUBBLICO DI CONNETTIVITÀ

72. Definizioni relative al Sistema Pubblico di Connettività

1. Ai fini del presente decreto si intende per:
   a) «trasporto di dati»: i servizi per la realizzazione, gestione ed evoluzione di reti informatiche per la trasmissione di dati, oggetti multimediali e fonia;
   b) «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;
   c) «connettività»: l'insieme dei servizi di trasporto di dati e di interoperabilità di base;
   d) «interoperabilità 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;
   e) «cooperazione applicativa»: la parte del Sistema Pubblico di Connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

73. Sistema Pubblico di Connettività (SPC)

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 Capo definisce e disciplina il Sistema Pubblico di Connettività (SPC), al fine di assicurare il coordinamento informativo e informatico dei dati tra le amministrazioni centrali, regionali e locali e promuovere l'omogeneità 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'interoperabilità 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:
   a) sviluppo architetturale ed organizzativo atto a garantire la natura federata, policentrica e non gerarchica del sistema;

b) economicità 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.

3-bis. Le regole tecniche del Sistema Pubblico di Connettività sono dettate ai sensi dell'articolo 71.

74. 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 qualità.

|SEZIONE II| SISTEMA PUBBLICO DI CONNETTIVITÀ SPC

75. Partecipazione al Sistema Pubblico di Connettività

1. Al SPC partecipano tutte le amministrazioni di cui all'articolo 2, comma 2.

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 altresì garantita la possibilità di connessione al SPC delle autorità amministrative indipendenti.

3-bis. Il gestore di servizi pubblici e i soggetti che perseguono finalità di pubblico interesse possono usufruire della connessione al SPC e dei relativi servizi, adeguandosi alle vigenti regole tecniche, previa delibera della Commissione di cui all'articolo 79.

76. Scambio di documenti informatici nell'àmbito del Sistema Pubblico di Connettività

1. Gli scambi di documenti informatici tra le pubbliche amministrazioni nell'ambito del SPC, realizzati attraverso la cooperazione applicativa e nel rispetto delle relative procedure e regole tecniche di sicurezza, costituiscono invio documentale valido ad ogni effetto di legge.

77. Finalità del Sistema Pubblico di Connettività

1. Al SPC sono attribuite le seguenti finalità:
   a) fornire un insieme di servizi di connettività condivisi dalle pubbliche amministrazioni interconnesse, definiti negli aspetti di funzionalità, qualità 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 qualità e la miglior fruibilità degli stessi da parte dei cittadini e delle imprese;
   c) fornire un'infrastruttura condivisa di interscambio che consenta l'interoperabilità 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 così 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.

78. 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 73, comma 3-bis***. **Le stesse pubbliche amministrazioni, ove venga loro attribuito, per norma, il compito di gestire soluzioni infrastrutturali per l'erogazione di servizi comuni a più amministrazioni, adottano le medesime regole per garantire la compatibilità con la cooperazione applicativa potendosi avvalere di modalità atte a mantenere distinti gli ambiti di competenza.**

2. Per le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, le responsabilità 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 (83).

2-bis. Le pubbliche amministrazioni centrali e periferiche di cui all'articolo 1, comma 1, lettera z), del presente codice, inclusi gli istituti e le scuole di ogni ordine e grado, le istituzioni educative e le istituzioni universitarie, nei limiti di cui all'articolo 1, comma 449, secondo periodo, della legge 27 dicembre 2006, n. 296, sono tenute, a decorrere dal 1° gennaio 2008

e comunque a partire dalla scadenza dei contratti relativi ai servizi di fonia in corso alla data predetta ad utilizzare i servizi «Voce tramite protocollo Internet» (VoIP) previsti dal Sistema Pubblico di Connettività o da analoghe convenzioni stipulate da CONSIP.

2-ter. Il CNIPA [oggi DigitPA] effettua azioni di monitoraggio e verifica del rispetto delle disposizioni di cui al comma 2-bis.

2-quater. Il mancato adeguamento alle disposizioni di cui al comma 2-bis comporta la riduzione, nell'esercizio finanziario successivo, del 30 per cento delle risorse stanziate nell'anno in corso per spese di telefonia.

79. 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 modalità 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 opportunità derivanti dalla evoluzione delle tecnologie;
   d) promuove la cooperazione applicativa fra le pubbliche amministrazioni, nel rispetto delle regole tecniche di cui all'articolo 71;
   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 82;
   f) dispone la sospensione e cancellazione dagli elenchi dei fornitori qualificati di cui all'articolo 82;
   g) verifica la qualità e la sicurezza dei servizi erogati dai fornitori qualificati del SPC;
   h) promuove il recepimento degli standard necessari a garantire la connettività, l'interoperabilità 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.

80. Composizione della Commissione di coordinamento del Sistema Pubblico di Connettività

1. La Commissione è formata da diciassette componenti incluso il Presidente di cui al comma 2, scelti tra persone di comprovata professionalità ed esperienza nel settore, nominati con decreto del Presidente del Consiglio dei Ministri: otto componenti sono nominati in

rappresentanza delle amministrazioni statali previa deliberazione del Consiglio dei Ministri, sette dei quali su proposta del Ministro per l'innovazione e le tecnologie ed uno su proposta del Ministro per la funzione pubblica; i restanti otto sono nominati su designazione della Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281. Uno dei sette componenti proposti dal Ministro per l'innovazione e le tecnologie è nominato in rappresentanza della Presidenza del Consiglio dei Ministri. Quando esamina questioni di interesse della rete internazionale della pubblica amministrazione la Commissione è integrata da un rappresentante del Ministero degli affari esteri, qualora non ne faccia già parte.

2. Il Presidente del Centro nazionale per l'informatica nella pubblica amministrazione (oggi DigitPA) 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 alla corresponsione di alcuna indennità, emolumento, compenso e rimborso spese e le amministrazioni interessate provvedono agli oneri di missione nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.

5. Per i necessari compiti istruttori la Commissione si avvale del Centro nazionale per l'informatica nella pubblica amministrazione, di seguito denominato: «CNIPA» [oggi DigitPA] e sulla base di specifiche convenzioni, di organismi interregionali e territoriali.

6. La Commissione può avvalersi, nell'ambito delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica, 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 può avvalersi, nell'ambito delle risorse finanziarie assegnate al CNIPA [oggi DigitPA] a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica, di consulenti di chiara fama ed esperienza in numero non superiore a cinque secondo le modalità definite nei regolamenti di cui all'articolo 87.

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

1. Il CNIPA [oggi DigitPA], 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 2, comma 2.

2. Il CNIPA [oggi DigitPA], 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.

82. Fornitori del Sistema Pubblico di Connettività

1. Sono istituiti uno o più elenchi di fornitori a livello nazionale e regionale in attuazione delle finalità di cui all'articolo 77.

2. I fornitori che ottengono la qualificazione SPC ai sensi dei regolamenti previsti dall'articolo 87, 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 [oggi DigitPA] 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 comma 1, 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'attività;
   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.

83. Contratti quadro

1. Al fine della realizzazione del SPC, il CNIPA [oggi DigitPA] 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 affidabilità complessiva del sistema, promuovendo, altresì, 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 77, 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 [oggi DigitPA]. Gli atti esecutivi non sono soggetti al parere del CNIPA [oggi DigitPA] e, ove previsto, del Consiglio di Stato. Le amministrazioni non ricomprese tra quelle di cui al citato art. 1, comma 1, del decreto legislativo n. 39 del 1993, hanno facoltà di stipulare gli atti esecutivi di cui al presente articolo.

84. 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 [oggi DigitPA], secondo le indicazioni da esso fornite, i piani di migrazione verso il SPC, da attuarsi entro diciotto mesi dalla data di approvazione del primo contratto quadro di cui all'articolo 83, comma 1, termine di cessazione dell'operatività della Rete unitaria della pubblica amministrazione.

2. Dalla data di entrata in vigore del presente articolo ogni riferimento normativo alla Rete unitaria della pubblica amministrazione si intende effettuato al SPC.

|SEZIONE III| RETE INTERNAZIONALE DELLA PUBBLICA AMMINISTRAZIONE E COMPITI DEL CNIPA [OGGI DIGITPA]

85. 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 il 15 marzo 2007, fatto salvo quanto previsto dall'articolo 75, 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 autorità amministrative indipendenti, possono aderire alla Rete internazionale delle pubbliche amministrazioni.

86. Compiti e oneri del CNIPA [oggi DigitPA]

1. Il CNIPA [oggi DigitPA] 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 modalità analoghe a quelle di cui all'articolo 83.

2. Il CNIPA [oggi DigitPA], al fine di fa vorire 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 83, comma 1, sostiene i costi delle infrastrutture condivise, a valere sulle risorse già previste nel bilancio dello Stato.

3. Al termine del periodo di cui al comma 2, 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.

4. Il CNIPA [oggi DigitPA] sostiene tutti gli oneri derivanti dai collegamenti in ambito internazionale delle amministrazioni di cui all'articolo 85, comma 1, per i primi due anni di vigenza contrattuale, decorrenti dalla data di approvazione del contratto quadro di cui all'articolo 83; per gli anni successivi ogni onere è a carico della singola amministrazione contraente proporzionalmente ai servizi acquisiti.

5. 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 85, comma 3, ne sostengono gli oneri relativi ai servizi che utilizzano.

87. 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, per l'avvalimento dei consulenti di cui all'articolo 80, 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 82.

|CAPO IX| DISPOSIZIONI TRANSITORIE FINALI E ABROGAZIONI

88. 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.

89. 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.

90. Oneri finanziari

1. All'attuazione del presente decreto si provvede nell'àmbito delle risorse previste a legislazione vigente.

91. 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).

3-bis. L'articolo 15, comma 1, della legge 15 marzo 1997, n. 59, è abrogato.
3-ter. Il decreto legislativo 28 febbraio 2005, n. 42, è abrogato.

92. Entrata in vigore del codice

1. Le disposizioni del presente codice entrano in vigore a decorrere dal 1° gennaio 2006.

DigitPA

Dipartimento per la Digitalizzazione
della Pubblica Amministrazione
e l'Innovazione Tecnologica

Formez PA

www.innovazionepa.gov.it