

CONTRIBUTI

Il Codice dell'amministrazione digitale

A cura del dirigente della segreteria dott. Francesco Conte

SOMMARIO

- | | |
|--|---------------------------------------|
| 1. Cosa è ed a cosa serve | 7. La PA digitale e la rete |
| 2. A chi si rivolge | 8. I tempi di applicazione |
| 3. Esclusioni e limitazioni | 9. Ultime novità |
| 4. PA digitale e nuovi diritti dei cittadini | 10. Il Protocollo informatico |
| 5. Definizioni | 11. DPR 28/12/2000, n. 445 - Estratto |
| 6. Gli strumenti della PA digitale | 12. CAD e processo telematico |

IL CAD (Codice amministrazione digitale)

Le riflessioni maturate durante alcuni recenti corsi frequentati presso la Scuola Superiore della Pubblica Amministrazione in tema di innovazione tecnologica, digitalizzazione ed *e-government* hanno favorito la stesura di questo breve memorandum-compilativo - non certo esaustivo di tutte le problematiche connesse al delicato tema trattato - sulla metodologia e tecnologia per la razionalizzazione e dematerializzazione dei processi amministrativi.

Le note seguenti, utili per un approccio al Sistema CAD, sono formulate sulla base delle norme del codice stesso e sull'elaborazione del materiale fornito ed indicato dai docenti della SSPA.

Il Codice dell'Amministrazione Digitale (D. Lgs. 7 marzo 2005 n. 82)

1. Cosa è e a cosa serve

Il *codice* è una specie di "costituzione del mondo digitale", che tiene conto di diritti e doveri e che contemporaneamente fornisce i principi operativi con cui tali diritti e doveri si possono concretizzare.

Il *codice* rende obbligatoria l'innovazione nella PA, da una parte dando ai cittadini il diritto di interagire sempre, dovunque e verso qualsiasi amministrazione attraverso Internet, posta elettronica, reti; dall'altra stabilendo che tutte le amministrazioni devono organizzarsi in modo da rendere sempre e comunque disponibili tutte le informazioni in modalità digitale.

In sostanza il *codice* ordina e riunisce molte norme già esistenti disponendone di nuove per nuovi servizi e nuove opportunità; esso ha creato insomma il quadro legislativo necessario per dare validità giuridica alle innovazioni.

2. A chi si rivolge

L'ambito di applicazione del CAD (art.2) va considerato sotto un duplice aspetto:

- chi adempie ai compiti individuati dal codice (Amministrazioni pubbliche, di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, Società, ecc.);
- a chi è rivolto un diritto o un servizio elettronico (Amministrazioni pubbliche, imprese, cittadini, soggetti privati, ecc.).

Sono attualmente allo studio presso il Consiglio della Magistratura Militare le varie modalità di applicazione/attuazione nell'organizzazione giudiziaria militare del C.A.D.

3. Esclusioni e limitazioni

L'applicazione del CAD è esclusa (art.2,co.6) per le attività connesse all'ordine e alla sicurezza pubblica, alla difesa e sicurezza nazionale, alle consultazioni elettorali.

Per quanto riguarda la Presidenza del Consiglio, è previsto, nello stesso articolo, che modalità, tempi e limiti di attuazione del CAD siano stabiliti con appositi decreti (v.ora, il DPCM 9 febbraio 2011); lo stesso vale per l'Amministrazione economico finanziaria (v.ora il DPCM 2 marzo 2011).

4. PA digitale e nuovi diritti dei cittadini

Nella Pubblica Amministrazione digitale i cittadini e le imprese hanno nuovi diritti che il codice precisa e definisce e che rende quindi effettivamente esigibili:

- i diritti dei cittadini e delle imprese a utilizzare l'informatica nei rapporti con lo Stato (*l'elettronica in aiuto alla democrazia*)- Art. 3 Diritto all'uso delle tecnologie;
- la partecipazione dei cittadini al procedimento amministrativo informatico (*trasparenza*) - Art.4;
- l'effettuazione di pagamenti con modalità informatiche (*semplificazione*)- Art.5;
- la diffusione dell'utilizzo della posta elettronica e in particolare di quella certificata (*semplicità d'uso ed economicità*)- Art.6;

- lo sportello unico per le attività produttive (*grande semplificazione*)-Art.10;
- la formazione, gestione, conservazione, trasmissione dei documenti (*vera rivoluzione nella gestione amministrativa*)- Capo III (artt.40-44 bis) e IV (artt.45-49);
- la forma e i contenuti dei siti delle amministrazioni (*utilità*)- art.50;
- la possibilità di inoltrare istanze e dichiarazioni per via telematica (*semplificazione*)- Art.65;
- il sistema pubblico di connettività (*semplificazione tecnologia e controllo dei costi*)- Capo VIII.

5. Definizioni – Art.1 CAD (aggiornato al 30 aprile 2012)

“

1. Ai fini del presente codice si intende per:

- a) **allineamento dei dati**: il processo di coordinamento dei dati presenti in piu' 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'identita' elettronica**: il documento d'identita' munito (di elementi per l'identificazione fisica) del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalita' di dimostrare l'identita' 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'identita' 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 e' 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 e' tratto;
- i-quater) **copia informatica di documento informatico**: il documento informatico avente contenuto identico a quello del documento da cui e' tratto su supporto informatico con diversa sequenza di valori binari;
- i-quinqies) **uplicato 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 conoscibilita' limitata**: il dato la cui conoscibilita' e' 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) **disponibilita'**: la possibilita' 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'ambito 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 e' 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 piu' documenti informatici, una data ed un orario opponibili ai terzi. »

6. Gli strumenti della PA digitale

Nella PA digitale i diritti elencati nel precedente punto 4 sono garantiti dalla disponibilità dei seguenti strumenti innovativi a cui il codice dà piena validità giuridica:

- *La posta elettronica certificata*

Ossia una e-mail che garantisce sia l'ora che la data di spedizione e di ricezione, provenienza (con una firma elettronica) e integrità del contenuto. Vale quanto una raccomandata con ricevuta di ritorno, costituendo una prova certa.

- *La firma digitale*

E' una firma elettronica che garantisce con sicurezza l'identificazione di chi firma e la sua volontà di firmare. Questa firma può sostituire sigilli, punzoni, timbri ecc. e dà validità giuridica a qualsiasi attestazione nei rapporti tra privati, tra privati e pubbliche amministrazioni e tra amministrazioni. Per rendere più sicura la firma elettronica questa deve essere certificata da un ente certificatore che risponda ai requisiti di legge e che si faccia garante dell'affidabilità della firma. Il codice regola tale certificazione.

- *I documenti informatici*

Un documento informatico, sottoscritto con una firma elettronica certificata, ha sempre e dovunque la stessa identica validità del documento cartaceo ad ogni effetto di legge e deve essere accettato da qualsiasi soggetto pubblico o privato. E' possibile quindi sostituire i documenti cartacei con documenti informatici. Le pubbliche amministrazioni possono raccogliere tutti i documenti relativi ad un procedimento in un fascicolo elettronico e devono comunicare ai cittadini interessati come accedervi, secondo quanto prescrive la legge sulla trasparenza (L.241/90). Il codice obbliga tutte le amministrazioni a gestire i documenti con sistemi informatici mediante il protocollo elettronico (certo e non modificabile) e l'archiviazione elettronica.

- *I siti Internet delle PA*

Quasi tutte le pubbliche amministrazioni hanno già i loro siti Internet, ma il codice ne rende obbligatorie alcune caratteristiche fondamentali: i siti pubblici devono essere accessibili da tutti, anche dai disabili, reperibili, facilmente usabili, chiari nel linguaggio, affidabili, semplici, omogenei tra loro. I siti Internet diventano la "porta" privilegiata per entrare nelle pubbliche amministrazioni e sono tenuti quindi a riportare alcuni dati necessari per orientarsi: l'organigramma per sapere chi fa cosa; gli indirizzi e-mail a cui rivolgersi per ciascuna necessità; l'elenco dei servizi forniti in rete; l'elenco di tutti i bandi di gara; l'elenco dei procedimenti svolti da ciascun ufficio con la loro durata e il nome del responsabile.

- *Le carte elettroniche*

La carta di identità elettronica e la carta nazionale dei servizi diventano lo strumento chiave per razionalizzare e semplificare l'azione amministrativa e sono regolate dal codice per essere uno strumento di autenticazione e di accesso ai servizi in rete della PA che sia universalmente valido in Italia, ma allo stesso tempo che contenga quei servizi e quelle utilità che ciascuna amministrazione territoriale giudichi utile per i propri cittadini.

7. La PA digitale e la rete

Nella PA digitale le amministrazioni cooperano tra loro e costituiscono una rete integrata di cui il codice definisce principi e finalità:

- *Il federalismo efficiente* (art.12) SPC - Il Sistema Pubblico di Connettività costituisce lo strumento che consente ai soggetti pubblici di dialogare, scambiare dati e documenti attraverso standard condivisi e canali sicuri: una rete fatta dalle reti delle pubbliche

amministrazioni, che mette in comunicazione PA centrale, PA locale, regioni e soggetti erogatori di servizi pubblici.

- *La cooperazione* (art. 10 e 64) - Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e comunicazione garantendo l'accesso alla consultazione, la circolazione, lo scambio di dati e informazioni, l'interoperabilità, ossia la capacità dei sistemi informatici di scambiarsi e di usare mutuamente informazioni anche se diversi.
- *La riorganizzazione gestionale e dei servizi* (art. 13) - Il codice lega strettamente l'utilizzo delle tecnologie al raggiungimento di obiettivi di efficacia, efficienza, economicità dell'attività amministrativa. Le pubbliche amministrazioni devono utilizzare le tecnologie in modo da razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, la modulistica, le modalità di accesso ai servizi.
- *La gestione informatica dei procedimenti* (art. 37) - Con il codice nasce il fascicolo informatico. Le pubbliche amministrazioni devono gestire i procedimenti utilizzando le nuove tecnologie e possono raccogliere in un "fascicolo digitale" atti e documenti relativi ad un procedimento anche se prodotti da amministrazioni diverse.
- *La trasmissione informatica dei documenti* (art. 50 e segg.) - Le amministrazioni possono comunicare e trasmettere documenti tra di loro in tempo reale. Il codice dà piena validità giuridica all'utilizzo della posta elettronica nella comunicazione tra uffici pubblici. Anzi è lo strumento con cui di norma le amministrazioni devono comunicare. Comunicazioni, atti e documenti trasmessi per e-mail tra uffici pubblici sono validi ai fini del procedimento amministrativo in tutti i casi in cui è possibile accertarne la provenienza e cioè se sono siglate con la firma digitale, oppure con protocollo informatico o trasmessi con posta certificata.
- *La disponibilità dei dati* (art. 53 e 60) - Le pubbliche amministrazioni devono rendere disponibili all'utilizzo da parte di altre amministrazioni i dati di cui sono in possesso, attraverso le tecnologie informatiche e telematiche. Ciascuna pubblica amministrazione titolare di dati è quindi tenuta a renderli accessibili, nell'ambito del Sistema Pubblico di Connettività, ad altri soggetti pubblici che ne fanno richiesta per lo svolgimento dei propri compiti istituzionali.
- *Le basi di dati di interesse nazionale* (art. 62) - Il codice individua come basi di dati di interesse nazionale un insieme di informazioni, omogenee per tipologie e contenuto. Le basi di dati di interesse nazionale costituiscono un sistema informativo unitario che

deve essere gestito, nel rispetto delle competenze dell'amministrazione che possiede i dati, garantendo l'allineamento delle informazioni e l'accesso da parte delle amministrazioni interessate nell'ambito del sistema pubblico di connettività.

8. I tempi di applicazione

La complessa normativa prevista dal Codice richiede tempi scadenzati (cfr. art.20, legge 15 marzo 1997, n.59, e successive modificazioni) per il suo recepimento, per adeguare processi e per formare il personale. La riforma quindi procede secondo una determinata tempistica.

9. Ultime novità.

Sulla Gazzetta Ufficiale n. 6 del 10 gennaio 2011 è stato pubblicato il Decreto Legislativo 30 dicembre 2010, n. 235; si tratta del provvedimento che ha concluso l' *iter* di riforma del Codice dell'Amministrazione Digitale (CAD), modificando il testo vigente del Decreto Legislativo n. 82/2005.

Altresì, il decreto-legge 9 febbraio 2012, n. 5, recante disposizioni urgenti in materia di semplificazione e di sviluppo, convertito in legge, 4 aprile 2012, n. 35, ha previsto, tra l'altro, con gli artt.6-ter, 47- ter, e 47- sexies, ulteriori modifiche ed integrazioni al CAD, in particolare:

- all'art. 5 è prevista, da parte delle pubbliche amministrazioni la pubblicazione sul proprio sito del codice IBAN e dei dati necessari per effettuare i versamenti;
- all'art. 15 è prevista la gestione in forma associata dei servizi ICT da parte dei comuni con popolazione fino a 5.000 abitanti;
- all'art. 63 è prevista l'erogazione dei servizi esclusivamente tramite i canali telematici, compresa la posta elettronica certificata, a partire dal 1° gennaio 2014.

Più in particolare con il citato D.Lgs. 235/2010 le modifiche - frutto della delega contenuta nell'art. 33 della Legge 18 giugno 2009, n. 69, con la quale il Parlamento ha dettato i principi e i criteri direttivi per una riforma del Codice dell'Amministrazione Digitale - hanno come obiettivo, da un lato, di adeguare il codice al veloce sviluppo tecnologico intervenuto

negli ultimi anni; dall'altro, dare maggiore efficacia a molte norme fino a questo momento rimaste disattese. Si riportano alcune delle novità emanate (ma tutto l'articolato è importante) e richiamate brevemente nei punti precedenti:

a) La copia informatica

Con l'introduzione delle lett. *i-bis*, *i-ter*, *i-quater* e *i-quinques* nell'art. 1 del CAD si è messo ordine nel dibattuto concetto di copia informatica. Partendo dall'assunto che forma "informatica" e contenuto del documento informatico sono due concetti da tenere distinti, si è arrivati a individuare varie categorie di copia informatica:

- “
- *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 informatico con diversa sequenza di valori binari;*
 - *i-quinques*) **uplicato informatico**: *il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario; ”*

b) La firma elettronica avanzata

- “ *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. ”*

Con l'aggiunta della nuova lettera *q-bis* dell'art 1, comma 1 del D.lgs. 82/2005 è stato reintrodotta, in Italia, il concetto di firma elettronica avanzata. Tale firma, già presente in Italia in seguito al recepimento della direttiva comunitaria 1999/93/CE, era stata eliminata nel 2005 con l'introduzione del CAD che non ne faceva più menzione, contenendo solo i concetti di firma elettronica, firma elettronica qualificata e firma digitale. Con l'introduzione

della firma elettronica avanzata si ha ora un quadro completo di firme elettroniche che tiene conto delle differenti soluzioni tecnologiche utilizzabili ai fini di garantire la corretta associazione di un documento ad un soggetto e l'integrità del documento stesso. Per una maggiore definizione è necessario comunque attendere le *Regole Tecniche* richiamate dall'art. 20 comma 3 e stabilite ai sensi dell'art. 71 del CAD.

Al pari della firma digitale e delle altre firme elettroniche qualificate, la firma elettronica avanzata permetterà ai documenti firmati di avere lo stesso valore probatorio riconosciuto alle scritture private (art. 2702 cod. civ.); non potrà essere utilizzata però per la sottoscrizione degli atti aventi ad oggetto beni immobili (art. 1350 c.c., nn. 1-12). In questi casi, viene obbligatoriamente richiesta la firma elettronica qualificata o la firma digitale (Art. 21 comma 2-bis, CAD).

c) Le nuove regole per il documento digitale (Artt. 20, 21, 22, 23-bis, 23-ter, 23-quater, 25 e 40)

Con la modifica degli articoli 20 e seguenti del CAD è stata rivista la sistematica complessiva delle norme relative al valore giuridico e probatorio del documento informatico e delle sue copie. L'idoneità a soddisfare il requisito della forma scritta e il valore probatorio del documento informatico sottoscritto con firma elettronica "semplice" restano sempre liberamente valutabili in giudizio, tenuto conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità del documento, mentre il successivo richiamo alle regole tecniche stabilite ai sensi dell'art. 71 viene allargato anche alla firma elettronica avanzata.

Proprio la necessità di aggiungere, accanto alla firma elettronica qualificata e alla firma digitale, la "nuova" firma elettronica avanzata ha dettato le modifiche dell'art. 21, che parifica le tre tipologie di firma relativamente al loro valore giuridico, stabilendo che solo per le scritture private di cui all'art. 1350 (primo comma, numeri 1-12) del codice civile è necessario ricorrere a una firma elettronica qualificata o alla firma digitale.

Il nuovo art. 22, poi, prevede grosse modifiche nell'assetto normativo relativo al valore giuridico delle copie informatiche di documenti analogici.

Interessanti, sono le novità in tema di documento amministrativo informatico contenute nel nuovo art. 23-ter. Per le copie informatiche di tali documenti, originariamente analogici, sarà necessaria un'attestazione di conformità rilasciata da un funzionario a ciò autorizzato.

Per le copie analogiche di documenti informatici, invece, viene introdotto il Timbro Digitale, ovvero un contrassegno generato elettronicamente e apposto in fase di stampa che consente la verifica automatica della conformità del documento analogico a quello informatico.

Infine, l'art. 23-*quater* conferma la modifica all'art. 2712 del Codice Civile, inserendo nel novero delle riproduzioni meccaniche anche quelle informatiche.

d) I dispositivi sicuri di firma e le procedure automatiche (Art. 35)

Con la modifica dell'art. 35 del CAD è stata ribadita la necessità che ogni dispositivo sia dotato di certificazione di sicurezza ed è stato individuato, nell'Organismo di Certificazione di Sicurezza (OCSI), l'ente deputato ad accertare la conformità di tali dispositivi ai requisiti di sicurezza richiesti per la creazione di una firma qualificata. Infine, è stata esplicitamente riconosciuta la validità delle certificazioni di sicurezza rilasciate da organismi all'uopo designati da un altro degli Stati membri e la cui investitura sia stata correttamente notificata alla Commissione Europea ai sensi dell'art. 11, paragrafo 1, lett. b, della Direttiva 1999/93/CE.

e) La conservazione dei documenti digitali (Artt. 44 e 44-bis)

Il D.lgs. 235/2010 ha introdotto alcune interessanti modifiche anche in tema di conservazione digitale.

Il nuovo comma 1-*bis* dell'art. 44 stabilisce, infatti, che il sistema di conservazione deve essere gestito da un responsabile [della conservazione] che lavori d'intesa con il responsabile del trattamento dei dati personali di cui all'art. 29 del D.Lgs. 196/2003 e, ove presente, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi. Inoltre, il successivo comma 1-*ter*, oltre a ribadire la possibilità che il processo di conservazione sia affidato in *outsourcing*, riconosce anche la possibilità che soggetti terzi certifichino la conformità di tale processo a quanto stabilito dall'art. 43 del CAD (Riproduzione e conservazione dei documenti) e dalle regole tecniche stabilite ai sensi dell'art.71 del codice medesimo.

Novità molto interessanti sono anche quelle introdotte dall'art. 44-*bis*. Secondo quanto stabilito da tale norma, i soggetti pubblici e privati che svolgono attività di conservazione dei documenti e di certificazione dei relativi processi, possono accreditarsi presso il DigitPa per conseguire il riconoscimento del possesso dei requisiti di livello più elevato in termini di qualità e sicurezza.

f) La Continuità operativa (Art. 50 bis)

L'articolo 50-*bis* introduce una piccola rivoluzione all'interno della PA italiana rendendo obbligatoria la definizione di un piano di continuità operativa e di un piano di *disaster recovery*.

In relazione ai nuovi scenari di rischio e alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni dovranno, quindi, predisporre piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e prevedere la duplicazione delle risorse informatiche necessarie per utilizzare i dati al fine del ritorno alla normale operatività.

La tendenza, o meglio, la necessità, è verso quindi un approccio (definito *Business Continuity*) ad un complesso di regole, metodi e tecnologie da implementare per garantire il ripristino non solo dei dati, ma anche dei sistemi informativi, delle risorse umane e strutturali colpiti da un evento disastroso.

g) PEC e invio di istanze e dichiarazioni alla PA (Artt. 6, 48, 65)

L'art. 6 del CAD viene integralmente riscritto dalla novella. Viene ulteriormente rafforzato l'obbligo per le pubbliche amministrazioni di utilizzare la posta elettronica certificata per tutte le comunicazioni in cui sia necessaria una ricevuta di invio e una di consegna con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata.

Inoltre, al fine di razionalizzare e uniformare il sistema di consultazione degli indirizzi di posta elettronica, viene disposta l'emanazione di un apposito regolamento a cura di DigitPA, sentito il Garante Privacy. Anche le modifiche dell'art. 48 del CAD hanno lo scopo di allineare il CAD su vari aspetti della posta elettronica certificata regolati successivamente al 2005 in altri atti normativi e regolamentari. La novità è **l'equiparazione dell'invio tramite PEC alla Notificazione per mezzo della posta** "*salvo che la legge disponga diversamente*" e non più nei soli casi previsti dalla legge. Infine, con la modifica dell'art. 65 del CAD si riconosce la Posta Elettronica Certificata come valido sistema di presentazione telematica di istanze e dichiarazioni alla PA: le istanze saranno valide, però, solo ove le credenziali di accesso alle PEC siano state rilasciate previa identificazione del titolare e ciò sia attestato dal Gestore di PEC nel corpo del messaggio o in un apposito allegato.

10. Il Protocollo informatico

Il protocollo informatico non è materia trattata direttamente dal Codice, in quanto già ampiamente disciplinata dai precedenti provvedimenti (a partire dal Testo Unico della documentazione amministrativa n. 445/2000, in cui il legislatore, art.1, co,1, lett.r, ha definito, tra l'altro, il protocollo informatico - quale sistema di gestione informatica dei documenti - 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 (artt. 40 BIS,41,47,57 BIS, 71)

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 susseguite 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.

11. DPR 28 dicembre 2000, n. 445

Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa

(Estratto - con indicazione del Capo, Sezione, e rubrica dei soli articoli riguardanti il protocollo informatico)

Capo IV

Sistema di gestione informatica dei documenti

Sezione I - Disposizioni sulla gestione informatica dei documenti

Art. 50 - Attuazione dei sistemi.

Art. 52 - Il sistema di gestione informatica dei documenti.

Art. 53 - Registrazione di protocollo.

Art. 54 - Informazioni annullate o modificate.

Art. 55 - Segnatura di protocollo.

Art. 56 - Operazioni ed informazioni minime del sistema di gestione informatica dei documenti.

Art. 57 - Numero di protocollo.

Sezione II - Accesso ai documenti e alle informazioni del sistema

Art. 58 - Funzioni di accesso ai documenti e alle informazioni del sistema.

Art. 59 - Accesso esterno.

Art. 60 - Accesso effettuato dalle pubbliche amministrazioni.

Sezione III - Tenuta e conservazione del sistema di gestione dei documenti

Art. 61 - Servizio per la gestione informatica dei documenti dei flussi documentali e degli archivi.

Art. 62 - Procedure di salvataggio e conservazione delle informazioni del sistema.

Art. 63 - Registro di emergenza.

Sezione IV - Sistema di gestione dei flussi documentali

Art. 64 - Sistema di gestione dei flussi documentali.

Art. 65 - Requisiti del sistema per la gestione dei flussi documentali.

Art. 66 - Specificazione delle informazioni previste dal sistema di gestione dei flussi documentali.

Sezione V - Disposizioni sugli archivi

Art. 67 - Trasferimento dei documenti all'archivio di deposito.

Art. 68 - Disposizioni per la conservazione degli archivi.

Art. 69 - Archivi storici.

Sezione VI - Attuazione ed aggiornamento dei sistemi

Art. 70 - Aggiornamenti del sistema.

12. CAD e processo telematico

In considerazione dell'importanza, e delle relative problematiche, che il tema delle notificazioni ha nell'ambito del processo telematico, è utile citare alcune fonti normative e regolamentari che dispongono l'adozione nel processo civile e penale di "protocolli" basati sulla tecnologia dell'informazione e della comunicazione, che hanno, appunto, all'interno del CAD le linee guida:

- Art. 51 del Decreto-legge 25 giugno 2008, n. 112, convertito con modificazioni dalla L. 6 agosto 2008, n. 133

Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione Tributaria.

- **Ministro della giustizia - D.M. 21 febbraio 2011 n. 44 - Pubblicato nella G.U. n. 89 del 18-04-2011)** *Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n.24;*
- **Ministro della giustizia - Provvedimento 18 luglio 2011** (Pubblicato per estratto sulla Gazzetta Ufficiale n. 175 del 29-7-2011) *Specifiche tecniche previste dall'articolo 34, comma 1 del decreto del Ministro della giustizia in data 21 febbraio 2011 n. 44, recante regolamento concernente le regole tecniche per l'adozione, nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2 del*

decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010, n. 24.

Sempre in tema di processo telematico è incentrato il recente decreto del Ministero dell'economia e delle finanze in data 26 aprile 2012, pubblicato sulla Gazzetta Ufficiale del 3 maggio 2012, n. 102.

Tale decreto (emanato sulla base dell'art. 39, co. 8, lett. B, del DL 6.7.2011, 98, conv. in legge 15.7.2011, n. 111) stabilisce (art. 2) le regole tecniche che permettono, nell'ambito del processo tributario, l'utilizzo della posta elettronica certificata per le comunicazioni e notificazioni degli uffici di Segreteria delle commissioni tributarie.

Le disposizioni (art. 10) trovano attuazione soltanto per le Segreterie delle commissioni provinciali e regionali dell'Umbria e del Friuli Venezia Giulia, ma, in seguito, con ulteriori decreti ministeriali, saranno gradualmente estese alle altre regioni.