



DocPaperless

Servizi, competenza e formazione per la digitalizzazione documentale

Considerazioni sulla disciplina relativa ai documenti informatici

Sono passati quattro anni dal 25 gennaio 2011, data di entrata in vigore del **Decreto Legislativo n. 235 del 30 dicembre 2010**, il quale modificando il **Codice dell'Amministrazione Digitale** (CAD - Decreto legislativo 7 marzo 2005 n. 82 s.m.i.), ha avuto il merito di introdurre sostanziali modifiche alla disciplina sul documento informatico e al processo di dematerializzazione.

In questo ultimo biennio sono arrivate le tanto attese **regole tecniche per l'attuazione omogenea ed uniforme** della norma primaria rappresentata dal CAD, regole tecniche che permettono di chiarire aspetti sulla validità sostanziale del documento informatico, sulla sua efficacia probatoria e sulle modalità di gestione, conservazione ed esibizione dei documenti.

Tra le regole tecniche emanate il **DPCM del 22 febbraio 2013**, in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali e la validazione temporale mediante marca temporale.

Il **DPCM 21 marzo 2013** per l'individuazione di 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

DocPaperless



Servizi, competenza e formazione per la digitalizzazione documentale

essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

Di rilievo fondamentale l'emanazione delle regole tecniche di cui al **DPCM 3 dicembre 2013** sia in materia di sistema di conservazione che per il protocollo informatico.

Da citare, inoltre, la **Circolare Agenzia per l'Italia Digitale n. 62 del 30 aprile 2013** contenente le linee guida per il contrassegno generato elettronicamente ai sensi dell'articolo 23-ter, comma 5 del CAD e la **Circolare Agenzia per l'Italia Digitale n. 65 del 10 aprile 2014** in merito alla modalità di accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici ai sensi dell'art. 44-bis, comma 1, del CAD.

Al predetto iter legislativo in materia di documento informatico si aggiunge un altro elemento fondamentale per l'attuazione del CAD il **DPCM 13 novembre 2014**, pubblicato sulla **Gazzetta Ufficiale n. 8 del 12 gennaio 2015**, il quale detta le **regole per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici sia per i privati che per le pubbliche amministrazioni**.

Le novellate disposizioni 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. Le novellate disposizioni, inoltre, si applicano ai privati nonché, ai sensi dell'art. 2, comma 4 del DPCM 13 novembre 2014, ad altri soggetti a cui è stata eventualmente affidata la gestione o la conservazione dei documenti informatici.

Il predetto DPCM entra in vigore l'**11 febbraio 2015 a trenta giorni** dalla pubblicazione in G.U. mentre i vari soggetti devono completare l'adeguamento dei propri sistemi di gestione informatica dei documenti alle regole del nuovo provvedimento **entro 18 mesi dall'entrata in vigore**.

È opportuno evidenziare che l'impianto normativo relativo al valore giuridico e probatorio dei documenti informatici in questi ultimi quattro anni si è evoluto in modo rilevante, passando da un contesto tecnico-normativo più rigido e definito tecnologicamente ad un **contesto più flessibile ed omogeneo** basato sui modelli organizzativi, sui processi, sui ruoli e le responsabilità, sugli standard per l'interoperabilità e soprattutto sui **principi di neutralità tecnologica e di libertà della forma del documento**.

È quest'ultimo l'aspetto più rilevante di tutta l'evoluzione normativa sul documento elettronico, in quanto è la base per permettere la vera interoperabilità tra Stati e la diffusione dell'e-business e dei servizi pubblici digitali.

A tal riguardo, non va oltremodo trascurato che l'attuazione futura del quadro legislativo di riferimento in Italia in merito al documento informatico andrà sempre più **coordinata con il quadro comunitario** grazie all'emanazione del **Regolamento n. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014**

in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, entrato in vigore il 17 settembre 2014 e direttamente applicabile in tutti gli Stati membri UE.

Il provvedimento comunitario permetterà, in modo progressivo da qui al 2018, di adottare nel mercato unico transfrontaliero e transettoriale europeo **un quadro tecnico-giuridico unico, omogeneo ed interoperabile** in ambito di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, documenti elettronici, nonché regole comuni per i servizi fiduciari nelle transazioni elettroniche, quali ad esempio la raccomandata elettronica o servizi di certificazione per l'autenticazione web.

In linea con la direzione intrapresa dalla disciplina italiana, lo stesso regolamento europeo eIDAS introduce un **nuovo approccio alla regolamentazione sulle transazioni commerciali elettroniche basato sui principi**, quali trasparenza e responsabilità, neutralità tecnologica, parità rispetto al documento cartaceo, regole di mercato basate su standardizzazione e quindi interoperabilità, costituzione di servizi fiduciari non qualificati o qualificati forniti da prestatori di servizi fiduciari (*Trust Service Providers TSP*), affidabilità e diligenza dei prestatori di servizi fiduciari con elevati requisiti di sicurezza ed attendibilità, copertura con polizza assicurativa da parte dei TSP in caso di danni provocati a persone fisiche e giuridiche a causa del mancato rispetto degli obblighi previsti dal regolamento e secondo determinati limiti.

Del regolamento europeo eIDAS si intende evidenziare un **principio base** disposto nell'**art. 46** rubricato *Effetti giuridici dei documenti elettronici* ovvero il principio della neutralità tecnologica e libertà della forma di un documento elettronico, dove secondo il regolamento stesso per documento elettronico si intende qualsiasi contenuto conservato in forma elettronica. L'art. 46 dispone che **ad un documento elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica.**

Per la valutazione del valore giuridico e della efficacia probatoria di un documento elettronico **conta**, quindi, **il livello di certezza dell'autenticità dell'origine e dell'integrità che il documento stesso è in grado di assicurare.** Ad esempio un documento su cui sono apposti una firma elettronica qualificata o un sigillo elettronico qualificato della persona competente per rilasciarlo (prestatori di servizi fiduciari qualificati) **gode della presunzione legale** di integrità dei dati e di correttezza dell'origine di quei dati a cui la firma o il sigillo elettronico qualificato sono associati.

Il medesimo principio di neutralità e libertà della forma è stato adottato dalla normativa italiana grazie proprio alle modifiche introdotte dal D.Lgs. 235/2010, per cui ai sensi dell'art. 20, comma 1-bis, del CAD **un documento informatico è liberamente valutabile dal giudice per la sua efficacia probatoria oltre che per la sua stessa assimilabilità alla forma scritta, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità**, ad eccezione di casi particolari come ad esempio l'atto pubblico informatico e fermo restando quanto disposto dall'art. 21 del CAD in merito al valore probatorio del documento sottoscritto.

Altro aspetto che merita attenzione nella normativa italiana sul documento informatico è **l'efficacia probatoria delle copie informatiche di documenti analogici e quella delle copie analogiche di documenti informatici**, in quanto la disciplina del CAD permette la distinzione di valore probatorio a seconda che si tratti di una copia autenticata o meno e dispone la distinzione di trattamento a seconda che si tratti di una copia di un documento amministrativo o meno o che si tratti di una copia di un originale analogico unico o non unico.

Ai fini della sostituzione ad ogni effetto di legge degli originali e dell'idoneità ad assolvere gli obblighi di conservazione previsti dalla legge la generazione della copia eseguita nel rispetto delle regole tecniche garantisce la piena equiparazione, mentre vi è una differenza in merito al pieno valore probatorio delle copie prodotte che può essere ottenuto solo quando le copie sono autenticate da un notaio o da altro pubblico ufficiale. Nei casi, invece, in cui le copie sono prodotte da altro soggetto, ad esempio dal soggetto che effettua la copia, anche attraverso la sottoscrizione con firma digitale, la loro validità è identica all'originale solo se la conformità delle stesse all'originale non viene espressamente disconosciuta in giudizio e ciò richiede un minimo di analisi e valutazione del rischio in caso di contenzioso.

La regolamentazione delle predette disposizioni definite nel CAD è stata finalmente completata con l'emanazione delle **regole tecniche di cui al DPCM 13 novembre 2014**, il cui contenuto è costituito al Capo I dalle definizioni ed ambito di applicazione, al Capo II dalle regole sul documento informatico, al Capo III dalle regole sui documenti amministrativi informatici, al Capo IV dalle regole sui fascicoli, registri e repertori informatici della pubblica amministrazione ed infine al Capo V dalle disposizioni finali.

Inoltre, le specifiche tecniche relative alle regole tecniche di cui al DPCM 13 novembre 2014, come nel caso del DPCM 3 dicembre 2013, sono raccolte in specifici allegati che ampliano il quadro di riferimento dell'attività di formazione, gestione e conservazione dei documenti informatici. In particolare, il Decreto richiama l'Allegato 1 "Glossario/Definizioni", l'Allegato 2 "Formati", l'Allegato 3 "Standard e Specifiche tecniche", l'Allegato 4 "Specifiche tecniche del pacchetto di archiviazione" e l'Allegato 5 "Metadati".

L'art. 3, comma 1, del DPCM 13 novembre 2014 disciplina le diverse modalità con cui gestire la **fase di formazione di un documento informatico**:

- a) redazione tramite l'utilizzo di appositi strumenti software;
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il **comma 2 dell'art. 3** stabilisce che il documento informatico assume la caratteristica di immodificabilità se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione. Il **comma 3 dell'art. 3** dispone che il documento informatico, identificato in modo univoco e persistente, sia memorizzato in un sistema di gestione informatica dei documenti o di conservazione la cui tenuta può anche essere delegata a terzi.

Tra le modalità indicate dal Legislatore meritano sicuramente una particolare sottolineatura quelle alla lett. c) e d) in quanto rappresentano una conferma fondamentale per l'inquadramento giuridico delle transazioni elettroniche.

Ciò deve portare in futuro ad un **maggiore consapevolezza, utilizzo e diffusione** delle operazioni di registrazione dei dati risultanti da transazioni o processi informatici e telematici attraverso la generazione di registri elettronici di dati che devono essere **“cristallizzati”** (resi immodificabili ed integri) tramite l'ausilio di strumenti di validazione (l'impronta hash, la validazione temporale tramite riferimenti temporali o marche temporali, il versamento al sistema di conservazione secondo le regole tecniche di cui al DPCM 3 dicembre 2013, l'apposizione di firme elettroniche, la trasmissione tramite PEC con ricevuta completa, ecc.).

Tale approccio va applicato sempre più **a tutti i processi informatici** di un'organizzazione pubblica o privata, in particolar modo se caratterizzati da una relazione con altri soggetti (clienti, fornitori, cittadini, ecc.).

Ad esempio si pensi alle procedure per la messa a disposizione di documenti su portali web, alle piattaforme di e-procurement o di pagamenti elettronici, all'e-commerce, alla fatturazione elettronica tra privati B2B e quindi alla messa a disposizione della fattura al destinatario attraverso piattaforme HUB che garantiscono contrattualmente la registrazione e la tracciatura delle operazioni eseguite dalle parti in gioco nella transazione commerciale.

Come già esposto in altri articoli, l'aspetto più importante del predetto ragionamento è quello di **regolamentare ed individuare contrattualmente la fase di formazione dei documenti in una transazione elettronica** al fine di renderla formalizzata tra le parti e correlata al quadro normativo di riferimento sulla formazione. Nella maggior parte dei casi, oggi, soprattutto in caso di affidamento all'esterno, viene contrattualmente gestita solo la fase di conservazione trascurando o lasciando nell'ombra quella della formazione dei documenti e della transazione, che peraltro risulta essere la fase più rilevante e critica in quanto rappresenta la fase iniziale del ciclo di vita di un documento informatico quindi la prima fase in cui si associa un grado di certezza giuridica e probatoria al documento e alla transazione stessa.

Di esempi di applicazioni se ne possono fare tanti altri. Una possibile applicazione è quella di integrare nei sistemi informativi nuove funzionalità di registrazione e cristallizzazione di dati e log, di generazione di registri elettronici che registrano i dati di un processo e creano delle piste di collegamento affidabili tra n documenti e n operazioni.

Ad esempio in un sistema informativo ERP (Enterprise Resource Planning) è possibile implementare un sistema di controllo contabile e creare delle piste di collegamento come indicato nella Circolare n. 18/E del

24 giugno 2014 attraverso la registrazione delle operazioni dell'intero processo contabile e la creazione di registri elettronici con l'utilizzo di hash e tecniche di cristallizzazione per mantenere nel tempo le registrazioni eseguite e completando il processo versando al sistema di conservazione pacchetti di versamento contenenti le registrazioni elettroniche.

Ciò permetterebbe di garantire nel sistema stesso di origine i riferimenti incrociati ed i requisiti di autenticità dell'origine, integrità e leggibilità della fattura e degli altri documenti appartenenti a tutti i processi di business rilevanti di un'azienda (vendite, acquisti, gestione magazzino, contabilità, ecc.).

A seconda delle diverse modalità di formazione di un documento informatico, i **commi 4, 5 e 6 dell'art. 3** dettano nello specifico le **operazioni per poter garantire le caratteristiche di immodificabilità e di integrità** al documento informatico.

Il **comma 7 dell'art. 3** ricorda l'importanza di associare almeno un riferimento temporale al documento informatico immodificabile ed il **comma 8** dispone di produrre l'evidenza informatica corrispondente al documento informatico immodificabile nei formati previsti nell'Allegato 2 del DPCM 13 novembre 2014.

Il **comma 9 dell'art. 3** è molto importante in quanto stabilisce che al documento informatico immodificabile vengano associati **i metadati che sono stati generati durante la sua formazione**. L'insieme minimo dei metadati, definiti nell'Allegato 5 al DPCM 13 novembre 2014, è costituito da a) l'identificativo univoco e persistente; b) il riferimento temporale di cui al comma 7; c) l'oggetto; d) il soggetto che ha formato il documento; e) l'eventuale destinatario; f) l'impronta del documento informatico. Eventuali ulteriori metadati possono essere definiti in funzione del contesto e delle necessità gestionali e conservative.

L'**art. 4, comma 1, del DPCM 13 novembre 2014** dispone le regole in merito alla produzione delle **copie per immagine su supporto informatico di documenti analogici** stabilendo l'importanza di produrre la copia mediante processi e strumenti che assicurino che il documento informatico (copia per immagine) abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

Il **comma 2 dell'art. 4** indica che la copia per immagine di uno o più documenti analogici può essere sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che effettua la copia ed ha la stessa efficacia probatoria dell'originale da cui è tratta a meno che la sua conformità all'originale non sia espressamente disconosciuta.

Il **comma 3 dell'art. 4** fornisce un contributo utile in merito alla **procedura operativa di attestazione di conformità** delle copie per immagine su supporto informatico di un documento analogico di cui all'art. 22, comma 2, del CAD. L'attestazione di conformità può essere inserita nel documento informatico contenente la copia per immagine o in alternativa può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. In entrambi i casi il

documento informatico così prodotto è sottoscritto con firma digitale del notaio o con firma digitale o firma elettronica qualificata del pubblico ufficiale a ciò autorizzato.

L'art. 5 del DPCM 13 novembre 2014 da un punto di vista operativo è una conferma di quanto già disposto dal CAD in merito ai **duplicati informatici di documenti informatici** disponendo che la generazione degli stessi avvenga mediante processi e strumenti che assicurino che il documento informatico ottenuto sullo stesso sistema di memorizzazione, o su un sistema diverso, contenga la **stessa sequenza di bit del documento informatico di origine**.

L'art. 6 del DPCM 13 novembre 2014 è molto importante in quanto disciplina **le copie e gli estratti informatici di documenti informatici**, indicando i formati idonei, richiedendo la garanzia di corrispondenza del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza del contenuto dell'originale e della copia. Anche in questo caso si può generare una copia anche firmata digitalmente dal soggetto che effettua la copia con identica efficacia probatoria, a meno che venga espressamente disconosciuta o generare una copia con pieno valore probatorio in quanto autenticata da un notaio o da un pubblico ufficiale a ciò autorizzato. Inoltre, così come nell'art. 4, sono regolamentate le due modalità per generare le attestazioni di conformità ed apporvi la firma digitale da parte del notaio o pubblico ufficiale.

L'art. 7 comma 1 del DPCM 13 novembre 2014 regola la fase di **trasferimento dei documenti informatici al sistema di conservazione** richiamando le regole tecniche ed il manuale del sistema di conservazione di cui al DPCM 3 dicembre 2013. Merita particolare attenzione il **comma 3 dell'art. 7** in quanto stabilisce un principio sacrosanto sulla *responsabilità per culpa in vigilando* del Produttore dei documenti che ha l'onere di verificare il versamento del pacchetto di versamento (PdV) al sistema di conservazione. L'art. 3 di fatto sancisce il seguente obbligo *“Il buon esito dell'operazione di versamento è verificato tramite il rapporto di versamento prodotto dal sistema di conservazione.”*

Ciò avvalorava ancor di più l'importanza di uno degli oggetti più rilevanti del processo di conservazione introdotti dal DPCM 3 dicembre 2013 il **rapporto di versamento (RdV)**, anch'esso un documento informatico, che rappresenta l'esito della presa in carico da parte di un sistema di conservazione e quindi **deve essere generato in tutti i processi di versamento** di qualsiasi ambito e tipologia documentale e messo nella disponibilità del Produttore, in modo che il Produttore stesso possa avere le informazioni esaustive, chiare e corrette sull'esito dell'operazione di versamento al sistema di conservazione.

L'art. 8 del DPCM 13 novembre 2014 disciplina le **misure di sicurezza** da adottare per la tenuta del documento informatico. In particolare il **comma 2 dell'art. 8** indica come riferimento per i soggetti privati l'adozione, quale modello di riferimento, di quanto previsto dagli articoli 50-bis e 51 del CAD e dalle relative linee guida emanate dall'Agenzia per l'Italia digitale. Da un punto di vista dei ruoli

organizzativi e delle responsabilità il predetto comma 2 dell'articolo 8 conferma la necessaria piena sinergia tra il Responsabile della Sicurezza ed il Responsabile della Conservazione.

Al **comma 3 dell'art. 8** viene confermato l'obbligo di conformità alle misure di sicurezza previste dagli articoli da 31 a 36 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196 e dal disciplinare tecnico di cui all'allegato B del codice Privacy. Da un punto di vista dei ruoli organizzativi e delle responsabilità il predetto comma 3 dell'articolo 8 conferma la necessaria piena sinergia tra il Responsabile del Trattamento dei dati personali ed il Responsabile della Conservazione.

Il Capo III è interamente dedicato alla regolamentazione del **documento informatico amministrativo** quindi è rivolto alle pubbliche amministrazioni.

L'**art. 9 ai commi 1, 2 e 3** stabilisce varie disposizioni in merito alla formazione del documento amministrativo informatico confermando l'importanza del **manuale di gestione** ai sensi dell'art. 5 del DPCM 3 dicembre 2013 sul protocollo informatico e l'identificazione e la gestione del documento amministrativo informatico nel **sistema di gestione informatica dei documenti** di cui al Capo IV del D.P.R. 28 dicembre 2000, n. 445, **comprensivo del registro di protocollo e degli altri registri** di cui all'art. 53, comma 5, del D.P.R. 28 dicembre 2000, n. 445.

Il **comma 4 dell'art. 9** prevede che le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD siano identificate e trattate come i documenti amministrativi informatici nel sistema di gestione informatica.

Il **comma 5 dell'art. 9** dispone le modalità con cui il documento amministrativo informatico può assumere le caratteristiche di immodificabilità e di integrità mentre il **comma 6** stabilisce i formati da adottare.

I **commi 7, 8 e 9 dell'art. 9** definiscono per il documento amministrativo informatico l'insieme dei metadati minimi ed eventuali ulteriori metadati aggiuntivi da associare al documento a seconda che i documenti siano soggetti a registrazione particolare, siano di tipo generale o appartenente ad una tipologia comune a più amministrazioni pubbliche. Il **comma 10**, infine, dispone per le pubbliche amministrazioni le regole da soddisfare nei casi di trasmissione telematica di documenti amministrativi informatici.

L'**art. 10 del DPCM 13 novembre 2014** in merito al documento amministrativo informatico regola la produzione delle copie su supporto informatico di documenti amministrativi analogici e la modalità di attestazione di conformità prevedendo l'apposizione della firma digitale del funzionario delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza.

L'**art. 11 del DPCM 13 novembre 2014** è rilevante nelle pubbliche amministrazioni perché definisce precise responsabilità in capo al responsabile della gestione documentale, ovvero, ove nominato, in capo al coordinatore della gestione documentale in merito alle operazioni di versamento al sistema di conservazione. In particolare, è rilevante la corretta interazione tra il sistema di gestione informatica documentale ed il sistema di conservazione facendo riferimento al sistema di classificazione e al piano di

conservazione e alla verifica del buon esito di versamento, creando quindi una forte correlazione tra manuale di gestione e manuale della conservazione. Dal punto di vista dei ruoli organizzativi e delle responsabilità viene confermata la necessaria sinergia tra il Responsabile della gestione documentale ed il Responsabile della Conservazione.

L'art. 12 del DPCM 13 novembre 2014 dispone in materia di **misure di sicurezza per la tenuta del documento amministrativo informatico**, quindi la necessità di un piano della sicurezza del sistema di gestione informatica dei documenti, nell'ambito del piano generale della sicurezza ed in coerenza con quanto previsto in materia dagli articoli 50-bis e 51 del CAD. L'articolo, inoltre, sottolinea l'importanza che il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale operi d'intesa con il responsabile della sicurezza e il responsabile del sistema di conservazione.

In ultimo, il Capo IV (artt. 13-16) è completamente dedicato alla regolamentazione della fase di formazione, del trasferimento al sistema di conservazione e alla disposizioni in materia di misure di sicurezza per la tenuta dei **fascicoli informatici**, delle **aggregazioni documentali informatiche**, dei **registri e repertori informatici** delle pubbliche amministrazioni.

Il presente breve approfondimento della norma sul documento informatico mostra come in questo biennio abbiamo assistito ad **una evoluzione molto dinamica ed imponente del quadro normativo sul documento informatico**, senz'altro positiva, ma senza dubbio molto rapida.

Per quanto predetto la dematerializzazione non è affatto un processo compiuto ma è un nuovo processo culturale agli albori che in questo 2015 richiede maturazione, consolidamento e soprattutto crescita della conoscenza e competenza.

I punti di attenzione in termini di **rispetto della conformità normativa, sicurezza, qualità ed affidabilità** sono ancora davvero di rilievo, in particolare in merito alla modalità con cui i soggetti pubblici e privati dematerializzano i propri documenti ed atti. La corretta gestione dei processi di dematerializzazione in conformità alla normativa vigente, la sicurezza dei processi e degli archivi, la protezione dei dati, soprattutto se sensibili e giudiziari, sono aspetti in cui è richiesta sensibilità, analisi, competenza, conoscenza e formazione continua degli addetti ai lavori oltre che investimenti nelle soluzioni tecnologiche, nelle infrastrutture e nei servizi da parte degli operatori di mercato.

Diffondere e comunicare con convinzione su quotidiani, magazine, media e social network termini quali digitalizzazione totale, addio alla carta, dematerializzazione di tutta la pubblica amministrazione, passaggio completo al digitale, rivoluzione digitale, economia digitale è assolutamente corretto per creare una cultura digitale, per informare, comunicare le nuove innovazioni e quindi attivare un percorso di *Digital*

Transformation al fine di rendere più competitivo il sistema Paese. Tuttavia non va mai dimenticata la competenza, la qualità e la sicurezza che queste procedure richiedono in particolare per la natura di alcune tipologie documentali e per alcuni settori.

Ad esempio nell'ambito delle pubbliche amministrazioni, molti soggetti non sanno realmente cosa significhi gestire documenti informatici amministrativi o gestire un fascicolo informatico di documenti appartenenti ad un medesimo procedimento amministrativo o a più amministrazioni o cosa significhi eseguire un corretto scarto o un versamento all'archivio di stato.

Passando ad un altro esempio concreto nell'ambito privato, invece, molti soggetti che dematerializzano documenti rilevanti ai fini tributari non sanno nemmeno cosa sia la dichiarazione ai sensi dell'art. 52, decimo comma, del D.P.R. 633/72 obbligatoria da parte del depositario outsourcer o non conoscono gli effetti e l'applicazione dell'art. 2215 bis del Codice Civile o come e quando devono assolvere l'imposta di bollo sulle fatture elettroniche alla luce della definizione della fattura elettronica stessa chiarita con la Circolare n. 18/E del 24 giugno 2014.

Per questo nel corso del 2015 è opportuno, ad avviso dello scrivente, puntare sull'approfondimento, sulla formazione, sulla conoscenza normativa e sui tempi di una corretta adozione, fermarsi quindi anche un attimo per riflettere su come si sta gestendo il piano di azione dell'Agenda Digitale italiana, sul suo coordinamento regionale e sulla corretta adozione dei processi da parte del mondo privato.

Un dato oggettivo è che la normativa di riferimento è ormai chiara e completa per l'attuazione, gli strumenti di validazione abilitanti i processi di dematerializzazione sono in gran parte da tempo applicabili (ad esempio firme digitali remote o con procedura automatica, firme elettroniche avanzata, firme grafometriche, data certa elettronica, riferimenti temporali, ecc.), l'auspicio, pertanto, è che i processi di digitalizzazione dei documenti di imprese, professionisti e pubbliche amministrazioni vengano avviati con il giusto approccio.

Il 1 gennaio 2016 il CAD compierà i suoi primi dieci anni dall'entrata in vigore. Tanta strada è stata percorsa anche se con alcuni fisiologici errori, grazie alla competenza, all'impegno e alla spinta di molti che hanno creduto in questa nuova disciplina, sia in Italia che in Europa, e che ringraziamo di cuore.

Ora che la strada è giusta e delineata è necessario attuare operativamente e concretamente le disposizioni ponendo attenzione anche ad **aspetti qualitativi** intesi come *compliance* normativa, aspetti contrattuali, garanzia della massima sicurezza e protezione dei dati, garanzia in merito ad un'effettiva vigilanza di AgID, in particolar modo per quegli ambiti e per quelle tipologie documentali che per loro natura lo richiedono.

A completamento delle considerazioni sopra esposte si consiglia di non dimenticare che la gestione della propria documentazione aziendale ed in generale la gestione delle proprie transazioni elettroniche sono processi *business-critical* e quindi vanno affrontati con la giusta serietà e sensibilità.

In conclusione, l'auspicio per il 2015 è che la pubblica amministrazione sappia e possa accedere alle risorse economiche e soprattutto riesca ad investire, in termini di competenza e efficienza, nell'innovazione e nel progresso che va sotto il nome della "dematerializzazione" e del "documento informatico".

Per il settore privato delle imprese e dei professionisti, l'auspicio è invece quello di iniziare a considerare davvero la dematerializzazione con una **visione diversa** ovvero considerandola non come un inutile obbligo legislativo che impone solo investimenti e quindi costi, ma come **un progresso** che se adottato con convinzione può fattivamente permettere di essere più competitivi nel mercato globale.

19 gennaio 2015

Fabrizio Lupone

Digital Compliance Advisor & Trainer

DocPaperless Norma e Tecnica dei Processi Digitali

Web www.docpaperless.com

Twitter @DocPaperless

Copyright - DocPaperless Norma e Tecnica dei Processi Digitali - Servizi, Competenza e Formazione per la Digitalizzazione Documentale™

Tutti i diritti sul presente documento, compresi l'adattamento totale o parziale, la riproduzione con qualsiasi mezzo e/o su qualunque supporto (ivi compresi i microfilm, i film, le fotocopie, i supporti elettronici o digitali), nonché la memorizzazione elettronica e qualsiasi sistema di immagazzinamento e recupero di informazioni, sono di proprietà dello studio Ing. Fabrizio Lupone e riservati.

DocPaperless



Servizi, competenza e formazione per la digitalizzazione documentale