La nascita dei centri di conservazione digitale

The author illustrates the most important points of the Codice dell'amministrazione digitale (Code of digital administration), which regulates the creation and the transmission of digital records in Italy since 2006 but does not cover preservation in public administrations. The author focusses on what is necessary for the correct operation of the Centro di Conservazione Digitale (Centre for Digital Preservation), points out the risks connected with the character of digital media and discusses practicable preservation policies. Centres for digital preservation can solve the problem because they can lower running expenses and guarantee good quality. Finally, the author describes the way in which such Centres need to operate in order to create an efficient system for the preservation of digital records.

1. La pubblica amministrazione digitale

L'emanazione del d.P.R. 11 febbraio 2005, n. 68, contenente le disposizioni per l'utilizzo della posta elettronica certificata, del d. lgs. 28 febbraio 2005, n. 42, che istituisce il sistema pubblico di connettività (SPC) e la rete internazionale della pubblica amministrazione, del d. lgs. 7 marzo 2005, n. 82, recante il codice dell'amministrazione digitale, conferma l'impegno dello Stato italiano per la realizzazione di forme avanzate di *e*-government[1]. Queste norme disegnano uno scenario in cui i cittadini, le imprese e le pubbliche amministrazioni potranno e dovranno utilizzare le tecnologie informatiche per comunicare tra di loro, erogare servizi, presentare istanze, consultare banche dati di interesse pubblico.

Il codice dell'amministrazione digitale, le cui disposizioni sono entrate in vigore il 1 gennaio 2006, riconosce ai cittadini e alle imprese alcuni diritti fondamentali tra cui la possibilità di trasmettere

[1] È dal 1997 che il legislatore italiano emana norme volte ad introdurre nella pubblica amministrazione le tecnologie dell'informazione e della comunicazione per:

- dare ai cittadini e alle imprese la possibilità di accedere per via telematica ai servizi pubblici e alle informazioni;
- consentire alle amministrazioni di reperire direttamente, con strumenti informatici, tutte le informazioni necessarie alla erogazione dei servizi richiesti dai cittadini e dalle imprese;
- promuovere l'integrazione tra i servizi di amministrazioni diverse.

alle pubbliche amministrazioni ogni atto e documento in formato elettronico.

> art. 3, comma 1, del codice dell'amministrazione digitale
> «I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni *centrali* e con i gestori di pubblici servizi *statali*»
> art. 4, comma 1, del codice dell'amministrazione digitale
> «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»
> art. 4, comma 2, del codice dell'amministrazione digitale
> «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».

Ovviamente, per poter esercitare questi diritti i cittadini e le imprese dovranno dotarsi di:

a) *Strumenti per l'autenticazione informatica*. Attualmente le amministrazioni pubbliche fanno uso di USER-ID e PASSWORD le quali, purtroppo, non garantiscono un elevato grado di sicurezza. L'art. 64, comma3, del codice dell'amministrazione digitale fissa al 31 dicembre 2007 la data oltre la quale non sarà più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni con strumenti diversi dalla carta d'identità elettronica (CIE) e dalla carta nazionale dei servizi (CNS).
b) *Strumenti per la produzione di documenti informatici*. L'art. 21 del codice dell'amministrazione digitale riconosce al documento informatico sottoscritto con firma elettronica qualificata (firma digitale) un valore giuridico equivalente a quello riconosciuto ad un documento cartaceo sottoscritto con firma autografa («ha l'efficacia prevista dall'art. 2702 del codice civile*»)*, mentre la forza probatoria di un documento informatico sottoscritto con firma elettronica (firma debole) è rimessa alla libera valutazione del giudice.

c) *Strumenti per la presentazione di istanze per via telematica.* L'art. 65 del codice dell'amministrazione digitale stabilisce che le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica sono valide se sottoscritte con una firma digitale il cui certificato è rilasciato da un Certificatore accreditato, oppure quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi. Le istanze e le dichiarazioni inviate con queste modalità sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.
d) *Strumenti per il pagamento on line degli oneri* dovuti alla presentazione di determinate istanze – ad esempio, le istanze in carta da bollo – o per la fruizione di particolari servizi. Ai sensi dell'art. 5, comma 1, del codice dell'amministrazione digitale, almeno le pubbliche amministrazioni centrali dovranno attivare tali sistemi di pagamento entro il 30 giugno 2007.
e) *Strumenti per la trasmissione e la ricezione di documenti informatici per via telematica.* Si tratta della posta elettronica certificata il cui utilizzo da parte delle pubbliche amministrazioni e dei privati è regolamentato dal d.P.R. 11 febbraio 2005, n. 68, e dal decreto 2 novembre 2005 del Ministero per l'Innovazione e le Tecnologie, recante le regole tecniche. L'utilizzo di una casella di posta elettronica certificata garantisce:
    - la riservatezza e l'integrità dei messaggi;
    - la determinazione certa delle date di spedizione e di consegna;
    - la protezione contro i virus informatici presenti nelle e-mail;
    - un'ampia informativa sull'esito di ogni spedizione.

Dal punto di vista delle pubbliche amministrazioni, l'attuazione delle norme sopra citate richiede un sforzo enorme in termini di organizzazione, revisione dei processi e informatizzazione. Per ricevere i documenti informatici trasmessi da cittadini, imprese e pubbliche amministrazioni, gli enti dovranno attivare un indirizzo di posta elettronica certificata istituzionale, esplicitamente dichiarato e pubblicato su un apposito indice telematico gestito dal CNIPA.

art. 6, commi 1 e 2, del codice dell'amministrazione digitale
«Le pubbliche amministrazioni centrali utilizzano la posta elettronica certificata, di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, per ogni scambio di documenti e informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata. Tali disposizioni si applicano anche alle pubbliche amministrazioni regionali e locali salvo che non sia diversamente stabilito»
art. 47 del codice dell'amministrazione digitale
«Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. (…) Entro il 1° gennaio 2008 le pubbliche amministrazioni centrali provvedono ad istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata per ciascun registro di protocollo, nonché ad utilizzare la posta elettronica per le comunicazioni tra l'amministrazione ed i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati».

Relativamente alle esigenze di interoperabilità e cooperazione applicativa su base informatica e telematica tra tutte le pubbliche amministrazioni, il d. lgs. 28 febbraio 2005, n. 42, istituisce il sistema pubblico di connettività (SPC), che è l'insieme di infrastrutture tecnologiche e regole tecniche per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione. Al SPC dovranno partecipare tutti gli enti di cui all'art. 1, comma 2, del d. lgs. n. 165/2001, contenente le norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, adottando soluzioni tecniche compatibili[2].

art. 50 del codice dell'amministrazione digitale
«Qualunque dato trattato da una pubblica amministrazione, 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 amministra-

[2] Sono escluse solo le pubbliche amministrazioni che esercitano le funzioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali.

> zioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo il riconoscimento di eventuali costi eccezionali sostenuti dall'amministrazione cedente. (…) 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'ente titolare dei dati predispone, gestisce ed eroga i servizi informatici allo scopo necessari, secondo le regole tecniche del sistema pubblico di connettività di cui al decreto legislativo 28 febbraio 2005, n. 42».

Le pubbliche amministrazioni, come i cittadini e le imprese, dovranno poter formare documenti informatici a valenza giuridica e forza probatoria; pertanto, esse dovranno dotarsi degli strumenti necessari per la generazione e la verifica di firme digitali.

> art. 34, comma 5 del codice dell'amministrazione digitale
> «Entro il 1° gennaio 2008 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».

Le disposizioni contenute nel codice dell'amministrazione digitale spingono decisamente le pubbliche amministrazioni verso il re-engineering dei procedimenti amministrativi con un'azione che comprenda anche la rilevazione e la revisione dei documenti prodotti o ricevuti nell'ambito dei processi analizzati allo scopo di valutare la possibilità e l'opportunità di sostituire gli atti cartacei con entità digitali equivalenti

> art. 15, comma 2 del codice dell'amministrazione digitale
> «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».
>
> art. 41 del codice dell'amministrazione digitale
> «Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vi-

gente. La pubblica amministrazione titolare del procedimento può raccogliere in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati».
art. 57 del codice dell'amministrazione digitale
«Le pubbliche amministrazioni provvedono a definire e a rendere disponibili anche per via telematica l'elenco della documentazione richiesta per i singoli procedimenti, i moduli e i formulari validi ad ogni effetto di legge, anche ai fini delle dichiarazioni sostitutive di certificazione e delle dichiarazioni sostitutive di notorietà».

2. Le principali problematiche connesse alla conservazione dei documenti informatici

La produzione di documenti informatici, la loro trasmissione e ricezione per via telematica, con le modalità descritte nel paragrafo precedente, obbligano le pubbliche amministrazioni a cercare soluzioni concrete per la formazione e la conservazione della memoria digitale. Questa è la fase più critica del processo di transizione dal documento cartaceo al documento informatico, che attualmente è oggetto di studi e ricerche sia a livello nazionale che internazionale. L'obiettivo è quello di riuscire a trovare le soluzioni per mantenere inalterate nel tempo le caratteristiche di autenticità, integrità, accessibilità e intelligibilità dei documenti informatici. E questo indipendentemente dall'evoluzione delle tecnologie, dai cambiamenti a cui l'informatica ci ha abituati, dal deterioramento (obsolescenza) dei materiali che costituiscono le memorie elettroniche e gli altri dispositivi del computer.

Le principali problematiche connesse alla conservazione dei documenti informatici sono sostanzialmente riconducibili a quattro fattori:

- obsolescenza dei supporti di memorizzazione
- vita relativamente breve delle firme elettroniche;
- obsolescenza dei formati elettronici;
- obsolescenza dei sistemi.

2.a) Obsolescenza dei supporti di memorizzazione

Il documento informatico è costituito da un insieme di valori binari registrati su un supporto di memorizzazione – ad esempio, un hard disk magnetico o un disco ottico – che, attraverso un processo tecnologico di lettura e decodifica, diventa rappresentativo di atti, fatti o dati giuridicamente rilevanti. Poiché qualsiasi materiale è soggetto a deteriorarsi nel tempo, anche i supporti di memorizzazione (media) non sfuggono a questa legge della natura; di conseguenza ogni tipo di media sarà caratterizzato da un tempo di vita più o meno lungo e, comunque sia, non illimitato. Per far fronte all'obsolescenza dei supporti di memorizzazione, il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA), nella deliberazione 19 febbraio 2004, n. 11, recante le regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali, ha affidato al Responsabile della conservazione il compito di «verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto[3] del contenuto dei supporti».

2.b) Vita relativamente breve delle firme elettroniche

La firma elettronica, generata con modalità conformi alla normativa vigente, è lo strumento che permette di produrre documenti informatici aventi forza giuridica equivalente ai documenti cartacei sottoscritti con firma autografa. La firma elettronica, però, è sostanzialmente diversa dalla firma autografa: può essere trasferita da un supporto ad un altro senza perdere di validità; è una sequenza binaria verificabile solo attraverso il computer; è diversa per ogni documento pur essendo generata dalla stessa persona; è caratterizzata da un tempo di vita relativamente breve. Quest'ultima caratteristica, come si può facilmente intuire, incide molto negativamente sul processo di conservazione dei documenti informatici.

[3] Per riversamento diretto si intende «il processo che trasferisce uno o più documenti da un supporto ad un altro senza alterare la loro rappresentazione informatica».

In primo luogo, la vita di una firma digitale è legata al periodo di validità del relativo certificato elettronico che è stabilito da Certificatore in funzione della robustezza delle chiavi e dei servizi a cui esse sono destinati; attualmente, un certificato utilizzabile per la generazione di firme elettroniche qualificate (firme digitali) scade dopo uno o due anni a decorrere dalla data di emissione. Il Certificatore è obbligato a tenere registrazione, anche elettronica, di tutte le informazioni relative ad un certificato qualificato per un periodo non inferiore a 10 anni dalla data di scadenza o revoca. Potrebbe quindi accadere che non si possa verificare la validità di una firma digitale apposta su un documento informatico prodotto in un passato recente (15 – 20 anni) per la mancanza del relativo certificato elettronico.

In secondo luogo, la firma elettronica è soggetta, come qualsiasi altra entità informatica, all'obsolescenza tecnologica che ne riduce la sicurezza fino ad un livello inaccettabile. L'art. 52 del d.P.C.M. 13 gennaio 2004, recante le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici, indica come soluzione per l'estensione della validità di un documento informatico, i cui effetti si protraggono nel tempo oltre il limite della validità della chiave di sottoscrizione, il rinnovamento delle garanzie di sicurezza e di integrità attraverso la generazione di una marca temporale prima della scadenza del certificato relativo alla firma elettronica apposta al documento. Naturalmente, questa operazione andrà ripetuta prima della scadenza della marca temporale e così via nel tempo. Si precisa che, ai sensi dell'art. 50 del d.P.C.M. 13 gennaio 2004, una marca temporale rimane valida per almeno 5 anni a decorrere dalla data di generazione e che è prevista la possibilità di ampliare tale periodo su richiesta dell'interessato.

2.c) Obsolescenza dei formati elettronici

Si definisce formato elettronico l'insieme dei codici e delle regole che permettono, a partire da una sequenza binaria, di rappresentare, con l'ausilio di hardware e software, il relativo l'oggetto informativo con lo stesso contenuto e nella stessa forma che gli ha dato l'autore. Purtroppo, l'evoluzione tecnologica fa sì che i formati vengano continuamente rielaborati ed ampliati per rendere disponibili funzionalità

sempre più avanzate. Può quindi accadere che dopo un certo tempo un formato non venga più supportato dalle versioni più recenti dei software e che quindi i documenti elettronici conservati in quel formato non siano più leggibili e rappresentabili all'utente con il contenuto e la forma originaria.

Per scongiurare questo pericolo sono state proposte due metodologie: l'emulazione e la migrazione. La prima prevede lo sviluppo, nell'ambiente tecnologico più attuale, di programmi capaci di emulare l'operatività dell'hardware e del software che furono utilizzati per la produzione dei documenti informatici conservati, mentre la seconda si basa sulla migrazione periodica della sequenze binarie corrispondenti ai documenti archiviati in modo da convertire i formati obsoleti in altri più attuali. La tecnica dell'emulazione permette di conservare gli atti informatici originali, ma appare di difficile applicazione vista la quantità e la varietà degli ambienti tecnologici che si possono utilizzare per produrli. Quella della migrazione, invece, appare più fattibile, ma ogni processo di riversamento sostitutivo[4] comporta inevitabilmente la perdita degli originali che vengono sostituiti con entità digitali diverse, ma che permettono di rappresentarli in modo identico.

Le disposizioni contenute nella deliberazione CNIPA 19 febbraio 2004, n. 11, indirizzano decisamente verso il metodo della migrazione, richiedendo al Responsabile della conservazione di firmare digitalmente l'insieme dei documenti trattati, o l'insieme delle loro impronte digitali[5], per attestare la regolare esecuzione del processo. Qualora la migrazione coinvolga documenti informatici sottoscritti con firma elettronica o la copia digitale autenticata di documenti car-

[4] Il processo di migrazione viene anche denominato riversamento sostitutivo, intendendo per esso «il trasferimento di uno o più documenti conservati da un supporto di memorizzazione ad un altro, modificando la loro rappresentazione informatica».

[5] L'impronta digitale di un file, o message digest, è una stringa binaria di lunghezza fissa generata applicando ad esso una funzione matematica, denominata *funzione di HASH,* che garantisce:

- l'unidirezionalità, cioè l'impossibilità di risalire al file partendo dalla sua impronta digitale;
- la resistenza alle collisioni, cioè l'impossibilità di generare una stessa impronta digitale a partire da due file diversi

tacei originali unici[6], oltre alla firma del Responsabile della conservazione è richiesta anche la firma di un pubblico ufficiale per attestare la conformità di quanto riversato al documento di origine.

È evidente la complessità del processo di conservazione digitale disegnato dal legislatore italiano. Il Responsabile della conservazione deve monitorare costantemente il livello di obsolescenza dei formati elettronici relativi ai documenti archiviati ed eseguire per ciascuno di essi il riversamento sostitutivo prima che sia compromessa la capacità di rappresentarli in modo fedele, firmando gli oggetti digitali prodotti e richiedendo la presenza del pubblico ufficiale per l'attestazione di conformità nei casi in cui questa è obbligatoria. Complessità che aumenta in modo esponenziale se si considerano anche le problematiche connesse alla scarsa longevità delle firme elettroniche, esposte nel precedente paragrafo 2.b).

2.d) Obsolescenza dei sistemi

La formazione e la conservazione della memoria digitale può avvenire solo con l'ausilio di un sistema che, al minimo, permetta di memorizzare, su supporti idonei:

- le unità documentarie e le unità archivistiche unitamente ai metadati che le descrivono ed esplicitano le relazioni esistenti tra di esse;
- i metadati sul soggetto produttore;
- i metadati necessari per la descrizione archivistica del fondo;
- gli strumenti tecnologici che realizzano la rappresentazione fedele dei documenti digitali.

Una qualsiasi forma di manomissione o di malfunzionamento di questo sistema può determinare la perdita di una parte del materiale documentario digitale conservato o impedirne l'accertamento dell'autenticità.

[6] Nella deliberazione CNIPA n. 11/2004 si distingue tra documenti cartacei originali unici e documenti cartacei originali non unici, intendendo per documenti cartacei 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.

Il sistema di conservazione digitale, quindi, deve essere basato su un impianto tecnologico altamente affidabile e sicuro, le cui componenti siano state in qualche modo "certificate" da un'autorità competente. Tra le sue funzionalità dovranno senz'altro figurare la produzione e l'archiviazione della documentazione elettronica attestante il regolare funzionamento dei singoli componenti hardware e software (file di log) e sufficiente per consentire la ricostruzione, la revisione e l'esame delle sequenze di operazioni che hanno riguardato il patrimonio documentario e informativo conservato (audit trail). Occorre, inoltre, che tale sistema sia predisposto per gestire i processi di migrazione che si renderanno necessari per effetto dell'obsolescenza tecnologica dei dispositivi hardware, del software di base, del software di gestione dei dati e del software applicativo. Prima o poi, infatti, il Responsabile della conservazione si troverà nella condizione di dover sostituire il software che realizza la gestione del complesso documentario digitale conservato, con una versione più recente oppure con un altro prodotto di nuova generazione. E quando questo accadrà, egli non dovrà dipendere da un fornitore e non dovrà essere vincolato ad una determinata piattaforma tecnologica. Al contrario, dovrà disporre degli strumenti necessari per accertare la corretta esecuzione del processo di migrazione e certificare l'equivalenza tra lo stato iniziale e lo stato finale del sistema.

3. La nascita dei Centri di Conservazione Digitale (Ce.Co.Di.)

Dall'analisi delle problematiche esposte nel paragrafo precedente, si deduce che per assicurare la conservazione della memoria digitale è necessario disporre: di un impianto informatico caratterizzato dal più alto livello di sicurezza ed affidabilità; di figure professionali altamente qualificate in materia di archivistica, informatica, diplomatica del documento contemporaneo e diritto; di procedure formalizzate e coerenti con gli standard internazionali relativi alla descrizione, conservazione e fruizione dei fondi archivistici. Gli enti produttori, considerate le attuali difficoltà economiche e carenze di organico, difficilmente potranno attivare al loro interno strutture adeguatamente attrezzate e dotate del personale necessario, e questo porterà inevitabilmente alla nascita dei cosiddetti "Centri di Conservazione Digitale (Ce.Co.Di.)" o "Depositi Digitali", cioè di strutture dedicate alla con-

servazione della memoria digitale di più soggetti produttori. D'altra parte, esistono già gli *archivi di concentrazione*, ovvero istituzioni che hanno «lo scopo primario di conservare e tutelare i complessi documentari realizzati da altri soggetti produttori». Tali sono l'archivio centrale dello Stato e gli archivi di Stato, che conservano i fondi prodotti rispettivamente dalle amministrazioni centrali dello Stato e dagli enti statali. È ragionevole ritenere che nel prossimo futuro queste istituzioni dovranno ampliare la gamma dei loro servizi per comprendere anche la conservazione e la fruizione della memoria digitale degli enti produttori; così come è molto probabile che gli enti locali di maggiori dimensioni, quali ad esempio le Regioni, daranno vita a poli archivistici in grado di garantire l'acquisizione e la conservazione dei complessi documentari informatici prodotti dagli enti ricadenti nel territorio di loro competenza.

L'attivazione di Centri di Conservazione Digitale è una soluzione che trova riscontro anche nel modello OAIS (Reference Model for an Open Archival Information System), che rappresenta lo standard di riferimento per l'archiviazione e la conservazione delle risorse digitali. Secondo tale modello, infatti, è possibile realizzare un'architettura di tipo "Federated Archives", in cui più sistemi OAIS indipendenti condividono una stessa interfaccia utente per consentire a una comunità globale di accedere a più depositi digitali, oppure un'architettura di tipo "Shared Resources Archives", in cui un sistema OAIS può gestire più depositi digitali di soggetti produttori diversi e può servire più comunità di consumatori. Gli schemi rappresentativi delle due architetture in questione sono riportati nelle successive figure 1 e 2.

Verso la costituzione, a livello di polo territoriale provinciale o regionale, di strutture dotate di personale qualificato e tecnologie avanzate per l'erogazione di servizi archivistici informatici, si è indirizzato anche il progetto di *e*-government DOCAREA, realizzato dal Servizio Informatica e Sistemi Informativi dell'Amministrazione Provinciale di Bologna e finalizzato alla comunicazione digitale nell'ente e fra enti.

Nell'ipotesi di attivare un Centro di Conservazione Digitale (Ce.Co.Di.), il processo di formazione e conservazione della memoria

digitale dei soggetti produttori che si avvalgono dei suoi servizi può essere articolato in quattro fasi:

a) fase preparatoria o preliminare;
b) fase della formazione della memoria digitale;
c) fase del trasferimento del patrimonio documentario digitale dal soggetto produttore al Centro di Conservazione Digitale;
d) fase della conservazione digitale e dell'accesso

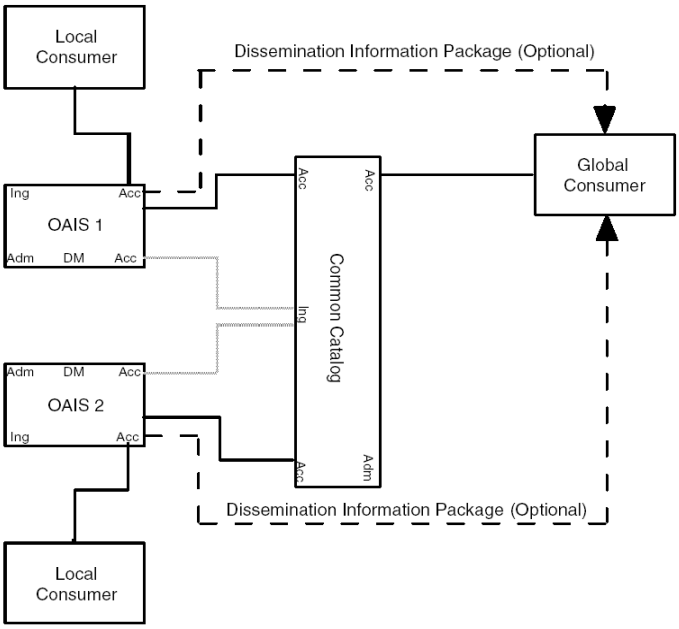

Fig. 1 – Schema architetturale di tipo "Federated Archives"[7]

[7] CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEM, *Reference Model for an Open Archival Information System (OAIS),* CCSDS 650.0-B-1, Blue book, 2002.

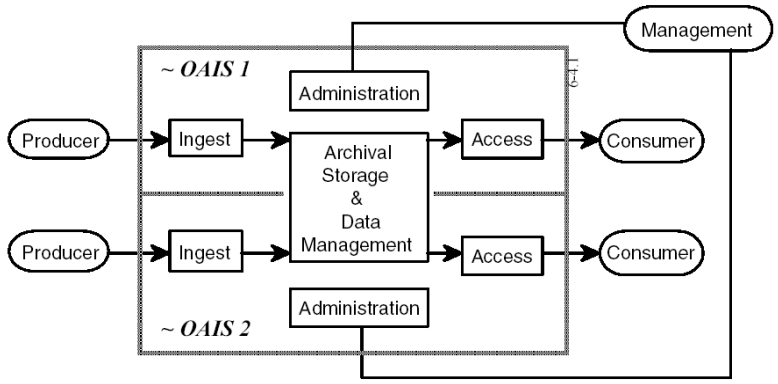

Fig. 2 – Schema architetturale di tipo "Shared Resources Archives"[8]

3.a) Fase preparatoria o preliminare

Per garantire la conservazione dei documenti informatici prodotti o ricevuti da un soggetto pubblico o privato durante lo svolgimento della sua attività, le strutture di archivio devono estendere la loro azione ai processi che attengono alla produzione documentaria, allo scopo di evitare che siano presentati al protocollo entità elettroniche non compatibili con un processo di conservazione digitale a lungo termine o mancanti delle necessarie informazioni di contesto.

Oltre alla predisposizione degli strumenti archivistici e organizzativi ampiamente richiamati nel testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (d.P.R. n. 445/2000) e nelle regole tecniche per il protocollo informatico (d.P.C.M. 31 ottobre 2000), rappresentati sostanzialmente dal titolario di classificazione, massimario di selezione e scarto, piano di conservazione dell'archivio e manuale di gestione dei documenti che implica la nomina del Responsabile del Servizio di protocollo informatico di cui all'art. 61, comma 2, del d.P.R. n. 445/2000, è necessario:

a) individuare i formati elettronici da utilizzare per la produzione dei documenti informatici;
b) verificare che siano state adottate le necessarie misure di sicurezza informatica;

[8] *Ibidem.*

c) verificare che il sistema di gestione informatica dei documenti (protocollo informatico) utilizzato dal soggetto produttore sia corretto sotto il profilo archivistico ed interoperabile con il sistema di conservazione digitale del Ce.Co.Di.;
d) effettuare il re-engineering dei procedimenti amministrativi con l'obiettivo di individuare e descrivere i documenti in relazione a ciascuna attività del soggetto produttore;
e) definire i tempi e le modalità di trasferimento delle unità documentarie e delle unità archivistiche dall'ente produttore al Ce.Co.Di.;
f) esplicitare l'insieme dei metadati che dovrà essere gestito con il sistema di protocollo informatico e successivamente trasferito al Ce.Co.Di.;
g) esplicitare le responsabilità per la formazione e la conservazione della memoria digitale;
h) definire le modalità di accesso e fruizione del complesso documentario digitale che sarà conservato presso il Ce.Co.Di.

In particolare, per quanto concerne la scelta dei formati elettronici da abilitare per la produzione dei documenti informatici, si devono tener presenti i requisiti tecnologici di seguito elencati.

- Sono da privilegiare i formati aperti, standard e documentati, perché assicurano l'indipendenza da uno specifico fornitore, l'interoperabilità tra sistemi eterogenei e un tempo di vita il più lungo possibile[9].
- Il formato elettronico deve consentire la rappresentazione del documento con lo stesso contenuto e nella stessa forma che gli ha dato l'autore, garantendo una fedeltà e una qualità grafica di livello adeguato.

[9] Nel modello OAIS (Open Archival Information System), un oggetto informativo digitale viene visto come l'insieme dei dati binari (data object) e delle informazioni che ne permettono la rappresentazione e la comprensione a livello utente (representation information). Per elaborare una representation information occorre conoscere il formato dell'oggetto informativo digitale trattato e questo è possibile solo se le sue specifiche sono state rese pubbliche (formato aperto); meglio ancora se queste specifiche sono state valutate e certificate come standard da un ente di normazione quale ISO, ANSI, W3C, IEFT, OMA, OASI, etc.

- Il formato elettronico deve permettere la rappresentazione digitale del documento indipendentemente dal contesto tecnologico in cui questa viene effettuata. In altri termini, è necessario avere la certezza che quello che viene rappresentato su computer sia identico, come contenuto e forma, a quello voluto e sottoscritto dall'autore. Il fatto che il documento venga prodotto in un certo contesto tecnologico e che si utilizzi un ambiente diverso per la sua rappresentazione non deve introdurre elementi di incertezza.

L'esecuzione della fase preparatoria richiede la più ampia collaborazione tra il Responsabile del Servizio di protocollo informatico del soggetto produttore e il Responsabile della conservazione che opera presso il Ce.Co.Di. Sono queste due figure, infatti, che dovranno garantire l'attuazione del principio della *custodia ininterrotta* secondo il quale «l'autenticità dei documenti può essere garantita solo provando l'esistenza, dal momento della loro produzione, di una serie ininterrotta di custodi responsabili»[10].

3.b) Fase della formazione della memoria digitale

Il documento archivistico deve essere considerato come parte costitutiva di un fondo, come elemento unico di un complesso organico, e non solo come entità singola. Pertanto, la conservazione dei documenti archivistici comporta la conservazione, oltre che dei documenti stessi, anche delle relazioni che li legano ai loro precedenti e susseguenti, delle unità archivistiche che li contengono e delle relazioni tra queste e le altre unità di pari livello o di livello superiore.

Nel caso dei documenti informatici, questo equivale a dire che il processo di conservazione digitale deve essere eseguito a partire dalla base informativa e documentaria prodotta sul sistema di protocollo informatico con l'esecuzione delle operazioni di protocollazione, classificazione e fascicolazione dei documenti, la gestione dei flussi documentali e dei procedimenti amministrativi. È l'insieme delle funzionalità del sistema di protocollo informatico che permette di rico-

[10] Ovviamente, se il Centro di Conservazione Digitale è una struttura del soggetto produttore, il Responsabile del Servizio di protocollo informatico e il Responsabile della conservazione possono essere la stessa persona.

struire i fascicoli informatici e le serie archivistiche digitali, collegandole alle attività sviluppate dal soggetto produttore.

La formazione della memoria digitale, quindi, avviene a cura del soggetto produttore, sotto il controllo del Responsabile del Servizio di protocollo informatico, utilizzando gli strumenti predisposti nella fase preparatoria e attuando il modello organizzativo e archivistico concordato preliminarmente con il Responsabile della conservazione.

3.c) Fase del trasferimento del patrimonio documentario digitale dal soggetto produttore al Centro di Conservazione Digitale

Nell'ipotesi che la struttura preposta alla conservazione della memoria digitale sia esterna al soggetto produttore, nasce il problema del trasferimento delle unità documentarie e delle unità archivistiche, con la relativa base informativa (metadati), dall'ente di origine al Centro di Conservazione Digitale.

In primo luogo, occorre stabilire *quando* eseguire il trasferimento. Da un lato, sappiamo che, a causa dell'obsolescenza tecnologica e della scarsa longevità delle firme elettroniche, le caratteristiche di autenticità, integrità e intelligibilità dei documenti informatici possono essere compromesse in un arco temporale relativamente breve se non vengono eseguite le opportune "attività di manutenzione"; dall'altro, poiché i fascicoli contengono i documenti relativi a un determinato procedimento amministrativo o, comunque sia, inerenti alla trattazione di uno specifico oggetto di competenza dell'ente produttore, essi si "completano" solo al momento della conclusione delle attività a cui si riferiscono. Pertanto, se il processo di conservazione digitale venisse eseguito al momento della "chiusura" dei fascicoli, ci si potrebbe trovare di fronte ad unità archivistiche "complete", ma "contenenti" unità documentarie digitali che hanno già perso le caratteristiche sopra citate. Una possibile soluzione potrebbe essere quella di eseguire il processo di trasferimento del patrimonio documentario digitale dal soggetto produttore al Centro di Conservazione Digitale in due tempi: prima le unità documentarie, con i relativi metadati, al momento della loro registrazione di protocollo, poi le unità archivistiche, con l'insieme dei metadati che le identificano e le collegano alle attività del soggetto produttore, al momento della loro "chiusura" da parte degli uffici di competenza. Il sistema di conservazione digi-

tale del Ce.Co.Di. dovrà fornire una visione unitaria ed organica del complesso di dati, documenti informatici ed unità archivistiche che sarà acquisito in più fasi, eseguite a distanza di tempo l'una dall'altra.

In secondo luogo, occorre stabilire *come* effettuare il trasferimento. Poiché esso comporta la movimentazione di entità digitali da un sistema ad un altro e il passaggio di "consegne" dal Responsabile del Servizio di protocollo informatico del soggetto produttore al Responsabile della conservazione che opera presso il Ce.Co.Di., è indispensabile che siano adottate soluzioni tecnologiche e procedure formalizzate che garantiscano, anche sotto il profilo giuridico:

- che quello che viene trasmesso dall'ente produttore coincida con quello che viene ricevuto dal Ce.Co.Di.;
- che i documenti informatici da sottoporre al processo di conservazione siano autentici, integri, accessibili e intelligibili;
- che l'insieme dei metadati, che accompagna il complesso documentario trasferito al Ce.Co.Di., sia completo e coerente con il disegno archivistico elaborato nella fase preparatoria;
- che sia attuato il principio della *custodia ininterrotta* sopra richiamato.

3.d) Fase della conservazione digitale e dell'accesso

Presso il Ce.Co.Di. si devono eseguire tutte le operazioni necessarie per la conservazione e la fruizione dei fondi digitali trasmessi dai soggetti produttori che si avvalgono dei suoi servizi.

Relativamente alle disposizioni emanate dal legislatore italiano in materia di conservazione dei documenti informatici, si rileva che esse introducono meccanismi che complicano pesantemente il lavoro del Responsabile della conservazione, il quale sarà costretto a tenere una sorta di "scadenzario" per tutte le firme elettroniche e le marche temporali associate ad ogni oggetto digitale archiviato nel Ce.Co.Di. Tra l'altro, il ricorso alla marcatura temporale per mantenere valido un documento informatico oltre la data di scadenza del certificato relativo alla firma elettronica ad esso apposta, crea problemi anche nella gestione dell'archivio corrente; infatti, viene spontaneo chiedersi come si deve comportare l'operatore dell'ufficio di protocollo che si vede recapitare un documento informatico sottoscritto con una firma

digitale il cui certificato elettronico scadrà dopo pochi giorni. Decisamente più efficace sembra essere la soluzione che affida al sistema e al Responsabile della conservazione l'onere di garantire nel tempo l'autenticità dei documenti informatici, indipendentemente delle firme elettroniche ad essi associate. Tale autenticità potrà essere dimostrata accertando la custodia ininterrotta, il regolare funzionamento di ogni componente del sistema di conservazione, la puntuale esecuzione delle operazioni di migrazione secondo procedure predefinite e formalizzate.

Fanno parte del processo di conservazione digitale anche le attività che attengono alla selezione e allo scarto dei documenti informatici, alla descrizione archivistica dei fondi conservati, alla loro valorizzazione e fruizione. Poiché la conservazione dei documenti informatici richiede l'esecuzione periodica di attività di controllo e migrazione che comportano un costo non trascurabile, i soggetti produttori dei fondi archivistici depositati nel Ce.Co.Di. avranno tutto l'interesse ad effettuare le operazioni di selezione e scarto con maggiore frequenza rispetto a quanto fanno oggi, pianificando per ogni tipo di documento e di unità archivistica, prima della loro produzione, un adeguato periodo di conservazione (massimario di selezione e scarto). Per quanto attiene alla descrizione archivistica e alla fruizione del patrimonio documentario digitale conservato nel Ce.Co.Di., si potrà utilizzare l'insieme dei metadati definito nella fase preliminare e adottare gli standard internazionali di riferimento, opportunamente ampliati per tenere conto delle peculiarità dei documenti informatici.

Si sottolinea, infine, il ruolo chiave del Responsabile della conservazione, che è chiamato a svolgere attività complesse, che richiedono un approccio di tipo multidisciplinare e che sono rilevanti sotto il profilo archivistico e giuridico. Si tratta di una nuova figura professionale, esplicitamente prevista dall'art. 5 della deliberazione CNIPA n. 11/2004, per la quale si stanno attivando percorsi formativi ad hoc, per ora rappresentati principalmente da master di specializzazione post laurea.

Stefano Pigliapoco[*]

[*] Università degli Studi di Macerata