



PIERLUIGI RIDOLFI

Nato a Ferrara nel 1934, si è laureato nel 1958 all'Università di Bologna in ingegneria industriale. Ha conseguito nel 1970 la libera docenza in "Teoria e Applicazione delle Macchine Calcolatrici". Dal 1974 è docente d'informatica all'Università di Bologna. Dal 1960 al 1993 in IBM Italia, è stato Direttore Centrale della Ricerca e dell'Innovazione Tecnologica e Presidente dell'IBM Semea Sud. Dal 1994 ha svolto incarichi di consulenza per importanti organismi pubblici e privati. È stato componente del collegio del CNIPA e ha fatto parte, come esperto, di vari organismi governativi: ha presieduto la "Commissione interministeriale per la gestione telematica del flusso documentale e dematerializzazione", la "Commissione interministeriale per l'impiego dell'ICT per le categorie deboli e svantaggiate", il "Gruppo di lavoro interministeriale per l'utilizzo della televisione digitale terrestre per l'e-government". Autore di una decina di libri in campo tecnologico, pubblicitario, gli è stato assegnato nel 2008 il Premio Eureka per l'innovazione tecnologica. È Presidente dell'Associazione Amici dell'Accademia dei Lincei.

Tecnologica e Presidente dell'IBM Semea Sud. Dal 1994 ha svolto incarichi di consulenza per importanti organismi pubblici e privati. È stato componente del collegio del CNIPA e ha fatto parte, come esperto, di vari organismi governativi: ha presieduto la "Commissione interministeriale per la gestione telematica del flusso documentale e dematerializzazione", la "Commissione interministeriale per l'impiego dell'ICT per le categorie deboli e svantaggiate", il "Gruppo di lavoro interministeriale per l'utilizzo della televisione digitale terrestre per l'e-government". Autore di una decina di libri in campo tecnologico, pubblicitario, gli è stato assegnato nel 2008 il Premio Eureka per l'innovazione tecnologica. È Presidente dell'Associazione Amici dell'Accademia dei Lincei.

IL NUOVO CAD. COMMENTI E PROSPETTIVE



a cura di
PIERLUIGI RIDOLFI

IL NUOVO CAD

IL NUOVO CAD. COMMENTI E PROSPETTIVE

9

COMMENTI E PROSPETTIVE

Atti del Convegno dell'8 luglio 2011 | Roma, Accademia dei Lincei



La Fondazione Siav Academy è il Centro per la Ricerca e lo Sviluppo dell'Innovazione Tecnologica nell'ambito di Siav Group. Attraverso il proprio Comitato Scientifico, costituito da alcuni dei più autorevoli esperti a livello internazionale, la Fondazione intende contribuire al dibattito e all'evoluzione scientifica, normativa e applicativa sui temi della dematerializzazione. La Fondazione, attiva nell'organizzazione di convegni e seminari formativi, opera anche nell'ambito dei Beni Culturali attraverso sponsorizzazioni e progetti dedicati alla conservazione e valorizzazione del patrimonio storico, culturale e artistico.

La Collana "Tecnologia dei processi documentali" rientra nelle attività pubblicitiche che la Fondazione promuove. Curata e coordinata dal Comitato Scientifico, con la supervisione puntuale del prof. Pierluigi Ridolfi, la Collana ha l'obiettivo di approfondire le più importanti e attuali tematiche che riguardano la gestione documentale, per quanto riguarda la normativa, le tecnologie, gli standard e le applicazioni.

in collaborazione con



PIERLUIGI RIDOLFI

9



Collana di Minigrafie
Tecnologia dei Processi Documentali

FONDAZIONE SIACV ACADEMY



FONDAZIONE SIAV ACADEMY

a cura di

PIERLUIGI RIDOLFI

IL NUOVO CAD COMMENTI E PROSPETTIVE

Atti del Convegno dell'8 luglio 2011 | Roma, Accademia dei Lincei

Contributi di

*Alfieri Voltan, Maria Guercio, Stefano Pigliapoco,
Benedetto Santacroce, Andrea Venturato, Marina Macario,
Michele Petrocelli, Vincenzo Gambetta, Andrea Lisi*

Collana di Minigrafie sulla

Tecnologia dei processi documentali

A cura di Pierluigi Ridolfi

© 2011 Fondazione Siav Academy - Edizione fuori commercio

È consentita la copia di qualunque parte di questo testo purché venga citata la fonte.

ISBN 978-88-97222-09-5



Collana di Minigrafie

Tecnologia dei Processi Documentali

INDICE

Introduzione

Alfieri Voltan, *Presidente Siav e Fondazione Siav Academy* **pag. 7**

Il nuovo CAD: luci e ombre

Pierluigi Ridolfi, *Presidente Associazione Amici Accademia dei Lincei e Comitato Scientifico Fondazione Siav Academy* **pag. 9**

La conservazione dei documenti digitali nel nuovo CAD e negli standard

Maria Guercio, *Università degli Studi di Urbino* **pag. 17**

Protocollare e archiviare la PEC e altri documenti informatici

Stefano Pigliapoco, *Università degli Studi di Macerata* **pag. 47**

Dalla firma digitale alla firma biometrica: quadro giuridico di riferimento per l'applicazione dei nuovi dispositivi di firma

Benedetto Santacroce, *Università degli Studi di Roma "Tor Vergata"* **pag. 57**

Dematerializzare il rapporto con i cittadini: una scelta organizzativa prima che tecnologica. Analisi progettuale

Andrea Venturato, *Fondazione Siav Academy* **pag. 67**

Dematerializzare il rapporto con i cittadini: una scelta organizzativa prima che tecnologica. Un'esperienza reale

Marina Macario, *Comune di Ciriè* **pag. 83**

L'informatizzazione dei processi di gestione del personale come strumento per la valorizzazione del servizio offerto: il caso MEF

Michele Petrocelli, *Direzione Centrale per i Servizi al Personale - Ministero dell'Economia e delle Finanze* **pag. 97**

La conservazione a lungo termine: tecnologie e soluzioni organizzative

Vincenzo Gambetta, *Consulente gestione dati, informazioni e contenuti e Direttore del periodico iged.it* **pag. 109**

Guida alla migliore scelta del responsabile "in outsourcing" per la conservazione digitale dei documenti

Andrea Lisi, *Presidente di ANORC* **pag. 125**

Il Convegno sul nuovo Codice dell'amministrazione digitale dell'8 luglio 2011 si è svolto nell'ambito delle iniziative promosse dall'Associazione Amici dell'Accademia dei Lincei, di cui la Fondazione Siav fa parte.

Alfieri Voltan

Introduzione

Alfieri Voltan

Presidente della Fondazione Siav Academy, inizia la propria carriera professionale nel 1974 nel settore dell'automazione aziendale. Successivamente collabora come consulente di Direzione presso Siemens Data, sviluppando sistemi di riconoscimento ottico di caratteri manoscritti (OCR), base tecnologica per la fondazione del gruppo Siav nel 1990. Sotto la sua direzione, Siav si è evoluta passando dalle tecnologie OCR all'archiviazione e gestione dei documenti in formato immagine, fino alle più recenti tecnologie di Business Process Management e Business Process Intelligence. Ha contribuito in maniera determinante allo sviluppo del mercato e delle tecnologie di cui oggi Siav è leader in Italia.

Saluto i presenti e ringrazio innanzi tutto l'Accademia Nazionale dei Lincei che ha acconsentito cortesemente di ospitare questo nostro convegno nella splendida sede della Villa Farnesina.

Scopo dei lavori di oggi è l'approfondimento di alcuni temi del nuovo Codice dell'amministrazione digitale, che rappresenta un passo avanti nello sforzo di creare le condizioni per la modernizzazione del nostro Paese.

Quest'anno, come noto, ricorre il 150° dell'Unità d'Italia. Io viaggio molto nel nostro paese, dalla Liguria alla Sicilia, dal Veneto alla Puglia, ed è stata per me una sorpresa vedere molte bandiere tricolori appese alle finestre delle case; ho sentito, o riscoperto, un diffuso senso di patriottismo e di amore e passione per il nostro Paese, in tutte le parti dell'Italia: e questo mi pare un segno positivo.

Sono convinto che questi valori, l'amore e la passione, debbano essere degli elementi ai quali noi dobbiamo cercare di riferirci, per cercare delle ragioni nuove del nostro agire. In un'Italia che sta attraversando un periodo critico, mentre è ancora difficile vedere delle vie d'uscita, io credo che cercare delle ragioni e

dei valori di riferimento forti sia un atteggiamento fondamentale per continuare la nostra missione, per andare avanti nonostante tutto, per cercare nei fatti una via d'uscita, per dare un contributo positivo al nostro Paese, per garantire un futuro migliore a noi e ai nostri figli.

Questo è il senso di quanto stiamo cercando di fare come Fondazione: promuovere una cultura dell'innovazione, attraverso la discussione, la presentazione di tematiche innovative, l'esame delle nuove normative che possono dare una spinta a queste innovazioni, oltre alla illustrazione di buone pratiche; insomma un contributo alla direttrice di evoluzione verso il futuro.

La Fondazione Siav Academy opera in questo senso anche tramite la pubblicazione dei lavori del proprio Comitato Scientifico: tramite il sito è possibile scaricare gratuitamente le Minigrafie, opere disponibili anche in formato cartaceo, che dibattono le tematiche relative al Codice dell'amministrazione digitale e la dematerializzazione della documentazione amministrativa; oltre a questo, sempre ad opera della Fondazione, è disponibile il sito di accesso pubblico e gratuito www.digita-lex.it, che riporta tutte le norme aggiornate e classificate relative al vastissimo campo dell'Amministrazione digitale.

È online una nuova rubrica, "Argomenti", dove vengono pubblicati articoli e contributi per una migliore comprensione delle normative e regole attuative del nuovo CAD.

Questa proiezione della Fondazione a promuovere l'innovazione mi auguro possa essere un buon viatico al quale riferirsi per cercare di sostenere la modernizzazione del nostro Paese.

Pierluigi Ridolfi

Il nuovo CAD: luci e ombre

Pierluigi Ridolfi

Nato a Ferrara nel 1934, si è laureato nel 1958 all'Università di Bologna in ingegneria industriale. Ha conseguito nel 1970 la libera docenza in "Teoria e Applicazione delle Macchine Calcolatrici". Dal 1974 è docente d'informatica all'Università di Bologna. Dal 1960 al 1993 in IBM Italia, è stato Direttore Centrale della Ricerca e dell'Innovazione Tecnologica e Presidente dell'IBM Se-mea Sud. Dal 1994 ha svolto incarichi di consulenza per importanti organismi pubblici e privati. È stato componente del collegio del CNIPA e ha fatto parte, come esperto, di vari organismi governativi: ha presieduto la "Commissione interministeriale per la gestione telematica del flusso documentale e dematerializzazione", la "Commissione interministeriale per l'impiego dell'ICT per le categorie deboli e svantaggiate", il "Gruppo di lavoro interministeriale per l'utilizzo della televisione digitale terrestre per l'e-government". Autore di una decina di libri in campo tecnologico, pubblicitario, gli è stato assegnato nel 2008 il Premio Eureka per l'innovazione tecnologica. È Presidente dell'Associazione Amici dell'Accademia dei Lincei.

Il 30 dicembre 2010 è stato emanato il Decreto Legislativo n. 235 che modifica e integra il CAD (Codice dell'amministrazione digitale), la cui prima versione risale al 2005 e che nel frattempo ha avuto vari aggiornamenti. Numerose le novità, tant'è vero che si parla di "Nuovo CAD": ci sono state variazioni in metà degli articoli e ne è stata aggiunta una decina. In totale il nuovo CAD consiste in 102 articoli, suddivisi, come prima, in IX Capi: esso contiene principi di ordine generale, rinviando ad apposito Decreto l'emanazione delle regole tecniche che disciplinano le singole materie (formazione, trasmissione, conservazione dei documenti informatici, firma digitale, protocollo, sistema pubblico di connettività, e così via). Nel Decreto legislativo sopra citato è prevista l'emanazione di una decina di questi Decreti, alcuni dei quali saranno del tutto nuovi, altri andranno a sostituire norme, di solito di rango inferiore, emesse precedentemente.

Il CAD si rivolge:

- alle Amministrazioni pubbliche;
- alle Società interamente partecipate da enti pubblici o con prevalente capitale pubblico;
- ai Gestori di servizi pubblici e organismi di diritto pubblico (per l'accesso ai documenti informatici);
- ai Privati (per tutto quanto riguarda i documenti informatici).

L'elenco delle amministrazioni pubbliche è vastissimo, in quanto comprende tutte le amministrazioni dello Stato, ivi inclusi:

- gli istituti e scuole di ogni ordine e grado e le istituzioni educative;
- le aziende ed amministrazioni dello Stato ad ordinamento autonomo;
- le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni;
- le istituzioni universitarie;
- gli Istituti autonomi case popolari;
- le Camere di commercio, industria, artigianato e agricoltura e loro associazioni;
- tutti gli enti pubblici non economici nazionali, regionali e locali;
- le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale;
- le Agenzie.

Non fanno parte delle amministrazioni pubbliche gli organi costituzionali e di rilievo costituzionale: pertanto il CAD non trova obbligatoriamente applicazione nella Presidenza della Repubblica, nei due rami del Parlamento, nella Corte Costituzionale. Per quanto riguarda la Presidenza del Consiglio è previsto che

modalità, tempi e limiti di attuazione del CAD siano stabiliti con appositi decreti; lo stesso vale per l'Amministrazione economico-finanziaria. Vi sono anche alcune restrizioni per quanto riguarda la difesa, la pubblica sicurezza, le consultazioni elettorali.

Si rammenta che i beneficiari del Codice sono, in modo diretto e indiretto, tutti i cittadini, che dovrebbero trarre vantaggio da una vera "Amministrazione digitale", cioè un'amministrazione pubblica i cui processi prevedono l'impiego delle tecnologie dell'informazione e della comunicazione con gli obiettivi di costare di meno, recuperare in efficienza, migliorare la qualità dei servizi. Ciò risulta evidente anche da una semplice scorsa ai principali argomenti trattati dal Codice:

- i diritti dei cittadini e delle imprese a utilizzare l'informatica nei rapporti con lo Stato (*l'elettronica in aiuto alla democrazia*);
- la partecipazione dei cittadini al procedimento amministrativo informatico (*trasparenza*);
- l'effettuazione di pagamenti con modalità informatiche (*semplificazione*);
- la diffusione dell'utilizzo della posta elettronica e in particolare di quella certificata (semplicità d'uso ed economicità);
- lo sportello unico per le attività produttive (*grande semplificazione*);
- la formazione, gestione, conservazione, trasmissione dei documenti (*vera rivoluzione nella gestione amministrativa*);
- la forma e i contenuti dei siti delle amministrazioni (*utilità*);
- la possibilità di inoltrare istanze e dichiarazioni per via telematica (*semplificazione*);
- il sistema pubblico di connettività (*semplificazione tecnologia e controllo dei costi*).

Sono tutti argomenti di grande rilievo, pensati nell'ottica di un miglioramento dell'efficacia e dell'efficienza della burocrazia dello Stato. Serviranno allo scopo? Io penso di sì: l'ottimismo sul futuro è funzione anche della valutazione del passato. Basta guardare indietro per vedere quali passi da gigante sono stati fatti negli ultimi anni. Certo, si poteva fare di più e meglio, ma la valutazione globale è del tutto positiva. Il confronto con gli altri Paesi europei ce lo conferma: nessuno ha un sistema così avanzato di posta elettronica, di firma digitale, di archiviazione sostitutiva, di connettività come il nostro.

Tornando al nuovo CAD, viene spontanea la domanda: c'è stato un miglioramento rispetto alla versione precedente? La risposta sostanzialmente è positiva, ma il giudizio va tarato anche in relazione alle regole tecniche: su alcuni argomenti si poteva fare di più e meglio.

Ho elencato nella tabella le principali innovazioni del nuovo Codice, con a fianco un'icona a faccina, per significare la mia personale valutazione.

	In ogni amministrazione pubblica un unico ufficio responsabile delle attività ICT, della razionalizzazione organizzativa e informatica dei procedimenti, dell'introduzione del protocollo informatico e del fascicolo elettronico
	Obbligo per le imprese e amministrazioni pubbliche di comunicare esclusivamente in modo telematico
	Enfasi sulla PE e sulla PEC
	Obbligo per le amministrazioni pubbliche di organizzarsi per il <i>disaster recovery</i>
	Una nuova disciplina per la conservazione e la copia di documenti
	Una nuova disciplina per l'accesso alle reti
	Creazione della nuova categoria dei "Conservatori accreditati"
	Quattro tipi di firma digitale

Otto, dunque, a mio parere, i nuovi argomenti importanti inclusi nel Codice: per quattro le norme sono chiare, per tre si poteva fare meglio, per una invece, a mio parere, si è creata una gran confusione.

Va benissimo imporre alle amministrazioni di modificare la propria organizzazione in modo da accentrare in un unico ufficio tutte le operazioni informatiche. Ci vorrà del tempo, ma si tratta di un'operazione necessaria in quanto strategica.

Fondamentale anche l'indirizzo a comunicare esclusivamente in modo telematico, con la posta elettronica semplice per gli atti privi di valenza giuridica e con quella certificata per quelli che attualmente richiedono l'invio di una raccomandata postale.

Per quanto riguarda le procedure di sicurezza per prevenire i danni provocati da eventi disastrosi è fatto obbligo alla amministrazioni di provvedere. Può sembrare una raccomandazione ovvia, ma non è così. Infatti, le soluzioni per garantire una ripartenza rapida dei processi porteranno inevitabilmente più amministrazioni a ricercare soluzioni comuni: ciò richiederà impegno e collaborazione tra le amministrazioni stesse, con uno stretto controllo dei costi. Una norma precisa al riguardo, come è quella contenuta nel Codice, è certamente di aiuto.

Fin qui va tutto bene.

Ora veniamo al primo punto in cui si poteva fare di più: la disciplina sulla conservazione e sulla copia dei documenti. Si tratta, in sintesi, di stabilire chi ha il potere di assicurare la conformità dei documenti archiviati in modo informatico agli originali cartacei da cui essi provengono. Mentre nel settore della pubblica amministrazione non c'è dubbio che qualunque funzionario abilitato allo scopo ha il potere di attestare tale conformità, in campo privato, a stretta applicazione della norma, occorre un notaio, documento per documento, il che rende praticamente

impossibile le operazioni. Era stato a suo tempo proposto dalla Commissione interministeriale sulla dematerializzazione di risolvere il problema qualificando *a priori* degli specifici processi di conversione dei documenti da cartaceo a informatico, affidando al pubblico ufficiale il compito di attestare *a posteriori* la corretta applicazione del processo piuttosto che la conformità del singolo documento: ma di ciò non c'è traccia nel nuovo Codice. Un'occasione mancata: che peccato! È ben vero che l'intervento puntuale del notaio elimina ogni rischio di possibili frodi, ma è altrettanto vero che se non si rischia un po' non si va avanti. Il concetto di valutazione del rischio e dei costi collegati, ben presente nel mondo industriale, sembra del tutto assente nelle procedure che vedono coinvolte le strutture amministrative pubbliche.

Su questa materia è in corso di pubblicazione la bozza di proposta di Decreto con le nuove regole tecniche, che vanno a sostituire quelle della vecchia, e per certi versi gloriosa, delibera Cnipa 11 del 2004. Da un esame preliminare il giudizio è in parte positivo: si tratta di un documento molto ben strutturato che però non aiuta a semplificare le procedure, secondo l'ottica sopra evidenziata.

Un altro campo in cui si poteva fare di più è quello relativo all'accesso alle reti. Va premesso che inizialmente l'identificazione informatica del soggetto richiedente era prevista mediante l'uso delle carte elettroniche (Carta di identità oppure Carta nazionale dei servizi): solo in via transitoria si potevano utilizzare tecniche diverse, come la coppia codice utente e parola chiave. Con il nuovo Codice le modalità di accesso vengono liberalizzate, cioè il metodo del codice utente e della parola chiave diventano la regola. In realtà lo sono già, però con una varietà di soluzioni tecniche fantasmagoriche. Non ci sono due amministrazioni che utilizzino lo stesso sistema, il che costringe il cittadino ad avere - e a ricordare - altrettante coppie di codici per ogni am-

ministrazione con la quale tiene rapporti. Alla distanza, ciò va a scapito della praticità e della sicurezza. Sarebbe stato opportuno prevedere delle linee guida di riferimento.

I conservatori accreditati sono una nuova categoria di operatori abilitati a operare con il massimo livello di professionalità in un settore delicato come quello dell'archiviazione della documentazione. Operatori con queste caratteristiche esistono già: si tratta di formalizzare in modo certo la loro capacità di interpretare correttamente le norme esistenti. Lascia però perplessi la possibilità che è stata loro data di certificare i processi. Non mi sembra prudente che allo stesso operatore vengano assegnati i ruoli di esecutore e di controllore: trattandosi di un campo molto innovativo, forse sarebbe stata opportuna una maggiore prudenza.

Quello che non va proprio è la nuova disciplina sulla firma digitale. Cercherò di sintetizzare in poche righe una materia assai complessa. I tre tipi di firma previsti dal vecchio Codice (elettronica semplice, qualificata e digitale) sono diventati quattro, perché si è aggiunta la firma avanzata. E fin qui poco male. Rammento che, in base alla direttiva europea sulle firme elettroniche, la firma avanzata è quella in cui viene direttamente collegata la firma con il documento informatico: essa ha valenza giuridica forte solo se accompagnata da un certificato qualificato e se realizzata mediante un dispositivo sicuro di firma, cioè quando è qualificata. La firma digitale è un caso particolare di firma qualificata, basato sul principio crittografico delle due chiavi. Nel nuovo Codice, inespugnabilmente, si stabilisce che la firma digitale è un caso particolare di firma avanzata (invece di qualificata) e che un documento firmato con qualunque tipo di firma avanzata, qualificata o digitale ha valenza giuridica piena, parificando così tipi di firma che sono in realtà ben diversi tra loro. Mi sfugge il razionale di questa novità che, per certi versi, mi sembra addirittura pericolosa.

In conclusione: con il nuovo Codice sono stati fatti dei passi in avanti: l'unico passo indietro è quello sopra segnalato della firma digitale. Nel complesso pertanto il giudizio è positivo. Ciò non toglie che vi siano dei punti critici che ne potrebbero pregiudicare la fattibilità.

Il primo sta nel presupposto che tutte le innovazioni sono previste a costo zero. Non faccio commenti, che sarebbero fin troppo ovvi: bisogna finanziare oggi le innovazioni per ottenere i risparmi di domani.

Un secondo punto critico sta nella mancanza di una prospettiva di formazione per il personale, senza la quale è impensabile che accada alcunché di innovativo. Forse questo è il problema maggiore che dovrà essere affrontato perché i vantaggi per il cittadino prospettati dal nuovo Codice diventino una realtà.

Maria Guercio

La conservazione dei documenti digitali nel nuovo CAD e negli standard

Maria Guercio

Professore ordinario di archivistica presso l'Università di Urbino e docente presso la SSPA nel campo della gestione informatica dei documenti. Collabora dal 1996 con gli enti di regolazione nella definizione di norme sulla gestione e conservazione dei documenti informatici. Svolge in questo campo un'intensa attività di ricerca nazionale e internazionale ed è autore di numerosi saggi e monografie. Ha vinto per il 2009 il premio internazionale Emmett Leahy - Information and Records Management Studies. Ha pubblicato numerosi articoli oltre al volume *Archivistica informatica* e al *Manuale di archivistica*, scritto insieme a Paola Carucci. Dirige la rivista "Archivi & Computer".

1. Premessa

Il ritardo accumulato negli anni nel nostro Paese nel campo della conservazione dei documenti digitali è stato molte volte stigmatizzato nel dibattito che ha coinvolto archivisti, informatici e giuristi¹. La questione è stata da un lato largamente sottovalutata da parte dei produttori e dei fornitori di soluzioni tecnologiche, da un altro ha scontato gli errori di prospettiva con cui il legislatore italiano l'ha affrontata, considerando il problema solo in termini di conservazione a breve-medio termine e circoscrivendolo per anni (almeno per il decennio 1994-2004) al nodo della validità giuridica della riproduzione sostitutiva dei documenti analogici. Anche dopo quella data le diverse componenti di un processo di conservazione non sono state peraltro compiutamente distinte e normate, se non, parzialmente, a seguito dell'arti-

¹ Per una trattazione più approfondita cfr M. Guercio, *Archivistica informatica*, Roma, Carocci, 2010, in particolare i capitoli 3 e 5, dedicati rispettivamente alla conservazione digitale e all'analisi del quadro normativo. Sul tema della conservazione è in corso di pubblicazione M. Guercio, *Conservare il digitale*, Bari, Laterza.

colo 44 del Codice dell'amministrazione digitale approvato con dlgs 82/2005. Il tentativo compiuto dal primo gruppo di lavoro sulla dematerializzazione costituito nel 2006 dal Cnipa ha fornito un primo quadro metodologico coerente sulle cui basi è stata elaborata (ma sfortunatamente non approvata) una bozza delle regole tecniche sulla conservazione previste ai sensi dell'articolo 71 del Codice medesimo (2007-2008) e di cui ha tenuto conto la riscrittura del CAD nel corso del 2010 (dlgs 235/2010, articoli 43, 44 e 44bis). È solo con le proposte di regolamenti attuativi in corso di discussione in questi mesi e di cui si tratterà ampiamente nel seguito che per la prima volta si tenta di fornire un quadro normativo sistematico in grado di contemperare le molteplici esigenze dei portatori di interesse in questo ambito (produttori, fornitori di software e di servizi, utenti finali) e le numerose difficoltà tecniche e organizzative (ma anche economiche) che la funzione conservativa implica.

Negli anni passati si sono, di fatto e troppo a lungo, confusi i piani e i temi della questione, trattando la disciplina delle copie, i modi e le responsabilità per formarle e verificarne la validità nella fase corrente come l'unico aspetto rilevante del processo di conservazione. Così facendo, i principi fondamentali (autenticità e affidabilità dei documenti e dei sistemi di conservazione), i metodi di riferimento e gli strumenti opportuni (strategie di migrazione o emulazione, metadati e formati, manuali di conservazione, gestione delle responsabilità, sviluppo e gestione di depositi digitali) sono rimasti inespressi sul piano giuridico e quindi privi di normalizzazione nelle pratiche di conservazione che nel frattempo si sono diffuse sia in ambito pubblico sia nel settore privato in forme largamente inadeguate rispetto ai requisiti funzionali indicati dalle raccomandazioni internazionali, pur rispettando la formalità del diritto vigente. L'espressione "conservazione a norma" rende immediatamente percepibile il nodo irrisolto: si sono stabilite regole da rispettare anche se que-

ste regole non sono state sufficienti a delineare un soddisfacente modello di conservazione. Fortunatamente gli archivi digitali fin qui prodotti e "conservati a norma" sono alquanto limitati nel numero e nella rilevanza qualitativa e, comunque, le disposizioni approvate, pur mancando di completezza e talvolta di chiarezza, non sono del tutto prive di indicazioni utili per i veri e propri processi di conservazione, anche se il loro obiettivo era meno ambizioso e generale. Come si è detto, le disposizioni del nuovo CAD hanno integrato e completato il quadro di riferimento, in particolare introducendo il principio dell'accreditamento e della certificazione dei soggetti (pubblici e soprattutto privati) che esercitano la funzione di conservazione, stabilendo l'obbligo di coordinare le diverse responsabilità in gioco all'interno della stessa struttura, imponendo nuovi strumenti in grado di documentare policy e procedure (il manuale di conservazione) e, *last but not least*, affrontando finalmente (con un incomprensibile ritardo) il nodo essenziale della continuità operativa dei sistemi informatici. Si tratta di aspetti che la regolamentazione tecnica in corso di discussione è destinata a definire con precisione, ma per fortuna anche con la necessaria flessibilità come si avrà modo di esaminare in seguito. A questo proposito merita osservare che l'intervento di regolamentazione in corso ha predisposto un sistema complesso di disposizioni che accompagnano il CAD² al fine di guidare a livello applicativo gli interventi operativi (regole tecniche in materia di formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni e di gestione del fascicolo informatico; regole tecniche sul sistema di conservazione ai sensi degli articoli 44 e 44 bis del CAD; regole tecniche per il protocollo informatico), inte-

² La documentazione è disponibile nel sito di DigitPA.

grandole con una serie di allegati tecnici tra cui un glossario che include voci non presenti nella normativa esistente e perfeziona la descrizione di termini rilevanti pur definite parzialmente in altri provvedimenti.

2. Principi e metodi per la conservazione di documenti digitali

Quanto affermato in precedenza ha naturalmente bisogno di essere innanzi tutto sostenuto sul piano concettuale e metodologico. In questa sede, ci si limiterà a considerare solo alcuni concetti chiave, senza la cui corretta individuazione e definizione si rischia di indebolire gravemente l'intero impianto regolamentare in materia. Un utile e concreto punto di partenza è costituito dal glossario reso disponibile – sia pure in forma provvisoria – dallo stesso gruppo di lavoro sulle regole tecniche³: la sua analisi costituisce un utile strumento per individuare e discutere brevemente i principi di fondo ai quali è opportuno ancorare la funzione di conservazione in ambiente digitale. Tra i termini che meritano di essere ricordati ci sono quelli che si riferiscono a concetti spesso utilizzati con significati difformi da diversi contesti disciplinari o addirittura di uso apparentemente comune, ma che in realtà sono cruciali sia in ambito giuridico sia in quello archivistico. La loro inadeguata comprensione nei processi applicativi rischia di ingenerare confusione e ambiguità, mentre una condivisione di significati consente di guidare con maggiore organicità i futuri interventi operativi. È il caso ad esempio dei termini di affidabilità, aggregazione documentale, autenticità e integrità, ma anche di archivio, ciclo di gestione, identificativo univoco e addirittura, come si è visto negli anni passati, di conservazione. Di seguito si riportano con qualche osservazione le definizioni dei termini citati proposte nella bozza di glossario:

³ Il glossario è disponibile nel sito di DigitPA.

- affidabilità (“caratteristica che esprime il livello di fiducia che l’utente ripone nel documento informatico”);
- aggregazione documentale informatica (“raccolta di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all’oggetto e alla materia o in relazione alle funzioni dell’ente”): si osserva che l’introduzione del termine è pregnante perché consente di gestire il legame tra i documenti nella forma di un legame originario e funzionale senza dover entrare nel merito di ulteriori più complesse distinzioni (ad esempio quella di fascicolo), non necessarie allorché si definiscono direttive generali per la conservazione⁴;
- archivio (“complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un soggetto produttore durante lo svolgimento dell’attività”);
- archivio informatico (“archivio costituito da documenti

⁴ È qui utilizzato un termine più corretto rispetto a quello di “fascicolo” (usato invece non del tutto a proposito nell’articolo 41 del CAD) allorché si tratta di indicare insiemi funzionali di documenti. Nella bozza di glossario il fascicolo (“raccolta, individuata con identificativo univoco, di atti, documenti e dati informatici, da chiunque formati, del procedimento amministrativo, nell’ambito della pubblica amministrazione”) è purtroppo indicato in generale limitatamente a quanto previsto nell’articolo, alquanto confuso su questo aspetto, del Codice, che non distingue tra il fascicolo inteso come sedimentazione di documenti a fini organizzativi e informativi all’interno del soggetto produttore e l’accorpamento di documenti per ragioni di trasparenza amministrativa ovvero in relazione alla gestione di specifici procedimenti. Il glossario avrebbe potuto in questo caso portare quel tanto di chiarezza che avrebbe consentito alle amministrazioni di gestire con semplicità ed efficienza il proprio sistema documentario rispetto alle esigenze specifiche della trasparenza. Solo per i privati il legislatore precisa che “è da considerarsi fascicolo informatico ogni aggregazione documentale, comunque formata, funzionale all’erogazione di uno specifico servizio o prestazione”. Sarebbe stato più corretto stabilire che il fascicolo è “un’aggregazione strutturata e univocamente identificata di atti, dati o documenti informatici funzionale all’esercizio di una specifica attività o di uno specifico procedimento” e sottolineare che “nella pubblica amministrazione, il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite nell’art. 41 del Codice.”

informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico”);

- autenticità (“caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche; l’autenticità può essere valutata analizzando l’identità del sottoscrittore e l’integrità del documento informatico”): si osserva che la definizione deriva senza dubbio dai principi del progetto internazionale InterPARES⁵ anche se il termine identità è qui usato in modo alquanto riduttivo perché riferito esclusivamente al sottoscrittore. In InterPARES e in generale nelle definizioni utilizzate nei contesti internazionali l’identità del documento riguarda tutte le caratteristiche significative che lo identificano univocamente;
- ciclo di gestione (“arco temporale di esistenza del documento informatico, del fascicolo informatico, dell’aggregazione documentale informatica o dell’archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo”);
- conservazione (“insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione”): il legislatore sembra finalmente consapevole della necessità di disporre di una definizione in grado di dar conto della complessità della funzione che comprende processi di gestione, ma anche strumenti e modelli organizzativi capaci di assicurare la persistenza dei documenti,
- identificativo univoco (“sequenza di caratteri alfanume-

rici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all’aggregazione documentale informatica, in modo da consentirne l’individuazione”⁶);

- integrità (“insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato nei suoi elementi essenziali”).

Le definizioni utilizzate dai nuovi provvedimenti, pur con qualche incertezza, forniscono un profilo concettuale condivisibile della funzione conservativa. L’autenticità è ad esempio definibile in modo apparentemente semplice come la capacità del documento di essere ciò che dichiara, senza falsificazioni e manipolazioni, riconducibile ai concetti di identità (identità dell’oggetto e delle sue relazioni rilevanti, ad esempio in rapporto agli altri documenti del fascicolo informatico, al procedimento amministrativo, all’ufficio di provenienza) e di integrità (riferito sia al contenuto e alla struttura del documento che agli elementi informativi che ne rappresentano le connessioni rilevanti).

Se identità e integrità costituiscono gli attributi qualificanti dei documenti autentici, il rischio maggiore è attribuito ai processi di trasmissione e di conservazione che, trasportando l’oggetto originario (inclusivo degli elementi informativi che lo collegano al sistema di produzione e di uso) al di fuori del suo con-

⁵ Cfr www.interpares.org.

⁶ Il termine in questione è ricorrente anche a livello internazionale ed è spesso utilizzato in modo ambiguo dato che non si specificano gli obiettivi: un identificatore potrebbe essere utilizzato a fini di integrità oppure per definire sequenze e correlazioni o ancora come elemento per il recupero del documento. In ambiente documentario uno stesso identificatore può essere multifunzione come nel caso del numero di protocollo che identifica non solo un documento, ma anche la sequenza cronologica collegandola a una data certa, a un soggetto produttore e a una serie molteplice di informazioni organizzative e gestionali in grado di assicurare certezza di acquisizione, integrità, correlazioni funzionali e altro ancora. Non è chiara la motivazione che spinge spesso la sperimentazione informatica verso un uso semplificato solo apparentemente del principio tradizionale perdendo per strada la ricchezza di strumenti consolidati nella tradizione. Nel glossario che si sta qui analizzando la definizione proposta consente entrambe le soluzioni.

testo amministrativo, documentario, tecnologico nello spazio (trasmissione) e nel tempo (conservazione) – rende inaffidabili i meccanismi che si basano sull'intangibilità del flusso di bit originario per formare documenti digitali imm modificabili. Più cresce la distanza cronologica che separa il documento dalla sua formazione più aumenta, infatti, la necessità di intervenire sugli oggetti per garantirne la leggibilità e l'intelligibilità rispetto alle criticità dovute all'obsolescenza tecnologica. È del resto ormai generalmente riconosciuto (e abbondantemente documentato) che l'autenticità in ambito digitale non è verificabile in termini di bit nel caso della conservazione a medio e lungo termine, ma può essere solo presunta sulla base dei requisiti cumulativamente rispettati da un sistema di conservazione: più alto è il numero dei requisiti previsti e rispettati, più alto è il grado di presunzione dell'autenticità. Anche la trasmissione mette in pericolo l'integrità, non tanto per quanto riguarda il contenuto informativo inviato quanto per la perdita dei riferimenti informativi cui quella risorsa è collegata nella fase attiva presso il soggetto che la produce e la gestisce.

Va poi affrontato in stretto collegamento con le considerazioni precedenti, un altro aspetto critico della conservazione, quello della validazione nel tempo del documento digitale, ovvero dei meccanismi e delle procedure che consentono di dichiarare autentico un documento (in quanto contenuto stabile imputabile con certezza a un autore per tutto l'arco temporale di esistenza del documento stesso) da parte di chi è autorizzato in un determinato sistema giuridico a produrre tale dichiarazione (l'autore medesimo, un pubblico ufficiale, un'autorità di certificazione o, addirittura, in base alla normativa vigente per alcune fattispecie documentarie, qualunque detentore del documento purché disponga di una firma digitale⁷). L'autenticazione interviene in una

molteplicità di fasi della gestione documentaria con funzioni e finalità diverse e per ragioni differenziate. Consiste in un metodo finalizzato a provare l'autenticità di un documento e in generale di qualunque oggetto digitale creato in un momento dato utilizzando strumenti o procedure di varia natura (firme elettroniche, sigillo informatico, contrassegno o timbro elettronico) finalizzate a rafforzare le garanzie di intangibilità e persistenza delle risorse conservate e i mezzi per la verifica. Il problema più impegnativo e sicuramente cruciale in termini di conservazione è quello relativo alla capacità di mantenere e gestire nel lungo periodo gli strumenti di validazione adottati. Le firme elettroniche e i sigilli informatici sono infatti essenziali nell'assicurare livelli adeguati di affidabilità nell'identificare la provenienza dei documenti. Sono essenziali anche nella stessa gestione dei processi conservativi in quanto consentono di verificare l'integrità delle risorse nelle fasi di trasferimento delle responsabilità anche se non garantiscono l'integrità nel caso in cui la risorsa sia oggetto di migrazione, ovvero nel caso in cui – come si è già ricordato – sia necessario modificare il *bitstream* originario. Non sono quindi mezzi idonei a sostenere, autonomamente dalle scelte organizzative, la verificabilità delle risorse a fini di conservazione a medio e lungo termine e in tutti i casi in cui i formati originari non possano essere mantenuti nel tempo. È per questa ragione che gli istituti di conservazione in Nord America non accettano in versamento documenti cifrati o firmati digitalmente anche se utilizzano temporaneamente meccanismi di cifratura e firma per gestire l'integrità dei trasferimenti tra produttore e deposito o tra depositi e dei pacchetti di archiviazione all'interno del deposito stesso. Altri strumenti di natura più complessa devono essere quindi adottati per consentire la verifica dell'autenticità dei documenti nel tempo.

È infatti accertato, nelle esperienze concrete di livello internazionale e confermato dalle ricerche di settore, che l'autenticità

⁷ Il tema è stato oggetto di ampio dibattito. Cfr <http://saperi.forumpa.it/relazione/il-nuovo-cad>.

delle risorse documentali è garantita e resa sostenibile dall'esistenza di un sistema di conservazione in grado di interagire (almeno al momento del passaggio di custodia dalla fase attiva a quella di deposito) con il sistema di formazione nel trattamento della integrità dei documenti e al fine della loro identificazione univoca e certa. A tal fine è indispensabile che siano gestite in modalità conservativa e rese disponibili nel tempo le cosiddette informazioni sulla rappresentazione dei documenti – così definite secondo lo standard ISO 14721 OAIS⁸ – relative ai metadati e agli elementi informativi predisposti in fase di formazione e nel corso dei processi di lavoro e custodia dei documenti e rilevanti per la loro comprensione anche in relazione al contesto originario di produzione e d'uso. In sostanza l'autenticità è verificabile se il sistema documentario e i modi concreti di produzione e gestione (incluso l'utilizzo di firme digitali e marche temporali) sono documentati in modo completo e accurato in tutte le fasi del ciclo di gestione dell'archivio e la conservazione digitale è gestibile a costi ragionevoli se le procedure sono pianificate e applicate sin dalla formazione dei documenti attraverso la creazione di un sistema di conservazione digitale.

A conferma di quanto finora sottolineato, meritano di essere ricordate le strategie proposte ai propri clienti da Adobe⁹ per la validità giuridica a lungo termine dei documenti digitali, da cui risulta con chiarezza la rilevanza dell'integrazione tra il sistema

⁸ Consultative Committee for Space Data Systems (CCSDS), Reference model for an open archival information system (OAIS): CCSDS 650.0-R-1, May 1999 (Red Book. Issue 1), http://ssdoo.gsfc.nasa.gov/nost/isoas/ref_model.html. Per la traduzione italiana cfr G. Michetti, Open Archival Information System/Sistema informativo aperto per l'archiviazione, ICCU, Istituto di studi per la tutela dei beni archivistici e librari dell'Università degli studi di Urbino, Roma, 2007. Lo standard è stato adottato dall'ISO come standard formale nel 2003 con il nome ISO 14721:2003 Space data and information transfer systems – Open archival information system – Reference model (OAIS).

⁹ Adobe PDF, Validità a lungo termine delle firme digitali. Strategie per garantire la validità a lungo termine dei documenti PDF con le firme digitali, http://www.adobe.com/it/security/pdfs/Wp_Digital_Sign.pdf.

di gestione corrente e il sistema di conservazione, ritenuta dalla società americana l'unica soluzione convincente in questo ambito. Tali strategie si riferiscono nello specifico all'incorporazione delle risposte di verifica e controllo da parte di chi deve verificare la validità del documento e prevedono più soluzioni:

- incorporazione nel pdf delle risposte sul controllo delle revocche con indicazione di data e ora dal server che le crea: l'esempio portato è quello di un consorzio di produttori farmaceutici che richiede il controllo incorporato come requisito per una soluzione “leggera”;
- incorporazione nel pdf di un controllo affidabile di data e ora inserito nel processo di produzione dell'impronta del documento: l'impronta viene trasmessa a un server in grado di generare indicatori di data e la risposta, inclusiva della data e ora, viene incorporata nel documento stesso, “riducendo così i requisiti dell'infrastruttura di convalida e massimizzando la portabilità degli stessi”, ma anche la necessità di ricorrere ad infrastrutture esterne per prolungare la validità nel tempo del documento dato che l'indicatore data e ora viene memorizzato all'interno del documento. L'esempio proposto riguarda il caso di un consorzio di consulenti finanziari che offre ai suoi membri un sistema di validazione di livello notarile utilizzando un server centrale dell'organizzazione in grado di apporre indicatori di data certa a tutti i documenti a loro volta sottoscritti dal notaio e di consentire quindi verifiche successive indipendenti;
- convalida di archivio: “internalizzazione del processo di autenticazione” mediante la registrazione dei processi di verifica e controlli di validità, revoca e indicatori di data e ora: i metadati sono conservati insieme ai documenti nel sistema di gestione dei documenti (è il caso di un tribunale che accetta documenti legali, moduli e prove e “non può

contare sul fatto che i certificati siano validi di per sé o sul fatto che una ...CA continui ad esistere [...]. Il risultato dei controlli viene documentato e memorizzato nei db e può essere referenziato nel sistema di gestione dei contenuti che ospita i documenti [...]. Il documento può essere considerato valido per un periodo indefinito, coincidente con l'esistenza dei sistemi di archiviazione"¹⁰.

Quest'ultima soluzione viene considerata da Adobe la più coerente con le esigenze di lungo periodo perché in grado di superare il rischio connesso a qualunque legame di dipendenza dalle infrastrutture tecnologiche. L'accento è spostato perciò sull'intero ciclo di gestione dei documenti e sulla necessità che le informazioni sulla validità dei documenti siano in primo luogo conservate e gestite dal soggetto produttore deputato alla loro tenuta più che dal fornitore di soluzioni tecnologiche. La conseguenza in termini conservativi è quella di assicurare la continuità tra le diverse fasi dell'archivio, soprattutto in termini di trasferimento delle informazioni descrittive relative al contesto documentario e giuridico nel passaggio di responsabilità della custodia.

Con particolare riferimento alla dimensione operativa la conservazione di documenti digitali si caratterizza più decisamente rispetto al mondo analogico in termini di gestione del rischio, da contenere con il continuo aggiornamento delle policy, delle attrezzature, degli standard di rappresentazione.

La conservazione, insomma, si configura come una funzione diffusa e persistente di cura del digitale (*digital curation*), la cui sostenibilità è garantita da:

- un'accurata documentazione delle attività e degli eventi che interessano la gestione degli oggetti digitali in tutte le fasi di gestione;

¹⁰ *Ibidem*.

- da interventi di mantenimento dei documenti e delle loro caratteristiche significative con specifica attenzione alla completezza e accuratezza degli elementi descrittivi/identificativi delle entità documentarie e delle relazioni di contesto che testimoniano la funzione del documento;
- dall'adozione di corrette e precoci politiche per gestire il trasferimento di custodia e la selezione.

La definizione di conservazione digitale proposta dallo standard ISO 14721 – Open Archive Information System (OAIS) conferma quanto finora qui sostenuto a proposito del peso della continuità dell'azione: “l'insieme dei principi, delle politiche, delle disposizioni e delle strategie finalizzate a prolungare l'esistenza di un documento o di una risorsa digitale grazie alla sua tenuta in condizioni adatte all'uso nella forma originale e/o in un formato persistente che garantisca l'integrità della configurazione logica e del contenuto”. In questa prospettiva i passaggi critici all'interno di un'organizzazione riguardano quindi:

- le policy interne a ciascuna organizzazione che nella nostra normativa sono riconducibili al manuale di gestione del sistema documentario (obbligatorio per le P.A. ai sensi del DPCM 30 ottobre 2001) e, più recentemente, al manuale di conservazione previsto dalla nuova regolamentazione tecnica (di cui la sicurezza costituisce solo una dimensione rilevante ma parziale);
- l'adozione di formati standard sin dalla fase di formazione dei documenti (al fine di ridurre gli interventi sul bitstream originario);
- l'individuazione di responsabilità certe, diffuse, coordinate e documentate.

L'adozione di un quadro concettuale condiviso – sia pure ridotto alle linee essenziali qui esaminate – consente di affrontare con

maggior concretezza e con qualche utile riferimento l'analisi della normativa esistente, oltre a permettere di identificare gli aspetti cruciali da approfondire nelle attività di ricerca applicata e nel concreto sviluppo delle soluzioni tecnologiche e organizzative.

Anche se molta strada resta da percorrere in questo ambito, i punti fermi ora ricordati si possono quindi considerare acquisiti. Si vedrà nel prossimo paragrafo se e come ne ha tenuto conto il legislatore italiano.

3. Il quadro normativo sulla conservazione

3.1 Aspetti generali

La normativa nazionale sulla conservazione dei documenti informatici ha conosciuto un percorso lungo e tortuoso che può essere distinto in due fasi di cui la seconda, recente, prende il via dal nuovo CAD. La molteplicità delle disposizioni messe in cantiere, riformulate, approvate e poi nuovamente riscritte è legata soprattutto alla difficoltà di trovare risposte certe e praticabili alle questioni ricordate nel paragrafo precedente in materia di verifica nel tempo della validità giuridica del documento e di immodificabilità dei contenuti informativi. Ha intralciato il percorso di per sé complesso anche la mancanza di chiarezza nell'individuare il nucleo centrale intorno al quale concentrare l'intervento normativo. Per troppi anni, infatti, si sono dedicate disposizioni a regolare la cosiddetta conservazione sostitutiva o a norma, che aveva il difetto di limitarsi quasi esclusivamente al processo di digitalizzazione di documenti analogici, al trattamento di documenti digitali provvisti di firma digitale e alla gestione conservativa di breve termine, ovvero a tematiche senza dubbio rilevanti per le scelte operative dei produttori, ma solo marginali rispetto al tema generale della conservazione.

Nello specifico, le esigenze principali affrontate dalla normativa

nella prima fase (dalla prima delibera Aipa n. 15 del 1994 fino alla deliberazione Cnipa 11/2004) includevano:

- l'individuazione di procedure per assicurare l'autenticità, l'integrità, la non modificabilità dei dati e dei singoli documenti conservati anche da un ente terzo per ragioni giuridiche e per un arco temporale limitato (senza quindi considerare i nodi tecnologici e organizzativi della conservazione a lungo termine di aggregazioni archivistiche e di interi archivi);
- la definizione di modalità per gestire i problemi di conformità all'originale di copie digitali sostitutive di documenti analogici al fine principale di destinare questi ultimi alla distruzione (previa autorizzazione della Direzione generale degli archivi) risparmiando spazi più che favorendo l'interoperabilità.

Negli ultimi anni i principi ispiratori del legislatore si sono progressivamente ampliati e comprendono oggi:

- una più chiara distinzione tra archiviazione/*storage* (intesa come semplice attività di memorizzazione su supporti digitali) e conservazione (finalizzata a rendere il documento non modificabile né deteriorabile e, quindi, capace di mantenere nel tempo le sue caratteristiche originarie di autenticità e integrità);
- la libertà dell'utente nel definire le modalità operative del processo (anche in risposta all'eccesso di dettagli tecnici e alla rigidità delle disposizioni, soprattutto di quelle precedenti la delibera 11/2004) e l'assenza di autorizzazioni preventive;
- il ricorso a meccanismi tecnologici per gestire l'immodificabilità (impronta del documento e apposizione all'insieme dei documenti da conservare di una marcatura temporale

connessa alla firma digitale da parte del responsabile della conservazione da utilizzare con funzioni di file di chiusura del nucleo di documenti da conservare ma anche come strumento di validità temporale opponibile a terzi ai sensi del DPCM 30 marzo 2009);

- una più ampia definizione del concetto di riferimento temporale opponibile a terzi per il quale si rendono disponibili strumenti diversi tra cui la marcatura temporale, la segnatura di protocollo, ma anche – ai sensi della nuova regolamentazione – le registrazioni in repertori, la posta certificata, la predisposizione di lotti per la conservazione;
- la individuazione delle modalità per l'esibizione dei documenti che tuttavia presenta ancora rilevanti criticità anche di natura economica, a partire dall'obbligo di ricorrere a contrassegni elettronici nel caso di esibizione analogica di documenti digitali;
- la identificazione dei compiti del responsabile della conservazione che includono la realizzazione secondo principi di sicurezza documentati di un sistema informativo relativo ai documenti digitali e la definizione e gestione dell'ambiente applicativo, con specifica attenzione alla tipologia dei documenti da conservare, alle copie di sicurezza e all'eventuale delega di funzioni a terzi.

La seconda fase ha preso decisamente e positivamente il via a partire dal dlgs 235/2010 che ha approvato il nuovo CAD e dalla regolamentazione in corso di elaborazione. Il CAD presenta un sistema complesso di disposizioni di valenza generale, mentre le regole tecniche (sulla formazione, trasmissione, conservazione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni e di gestione del fascicolo informatico; sul sistema di conservazione ai sensi

degli articoli 44 e 44 bis del CAD; per il protocollo informatico), sono destinate a svolgere un ruolo di guida a livello applicativo.

3.2 Il Codice dell'amministrazione digitale

La nuova versione del CAD include alcune importanti novità in materia di conservazione sia grazie a quanto specificatamente stabilito dagli articoli 43, 44 e 44bis, sia per quanto contenuto in altre disposizioni. Data la complessità del decreto ci si limiterà a esaminare solo quegli articoli che hanno un riferimento esplicito alla conservazione o regolamentano aspetti di rilievo cruciale in questo ambito.

L'articolo 43 (conservazione dei documenti) – fermo restando l'obbligo previsto dall'articolo 41 comma 1 di produrre i documenti delle pubbliche amministrazioni in forma digitale – ne prescrive la tenuta nel tempo nella medesima modalità per tutti i casi per i quali sia “prescritta la conservazione per legge o regolamento”, anche qualora gli originali siano stati formati su altri supporti: la loro validità giuridica e rilevanza è assicurata a condizione che “la riproduzione e la conservazione nel tempo siano effettuate in modo da garantire la conformità dei documenti agli originali nel rispetto della specifica regolamentazione tecnica”, fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi tutelati (pubblici o privati dichiarati di notevole interesse storico).

L'articolo 44 (requisiti per la conservazione dei documenti informatici), dopo aver confermato quanto già stabilito dal CAD nel 2005 – ovvero che il sistema di conservazione dei documenti informatici garantisce l'identificazione certa del soggetto che ha formato il documento o che lo ha acquisito, l'integrità del documento e la leggibilità e agevole reperibilità dei documenti stessi e delle informazioni identificative inclusi i dati di registrazione e classificazione originari e il rispetto delle misure di sicurezza – introduce due nuovi importanti commi: il comma 1-bis, che prescrive la collaborazione tra i responsabili rispettivamente del

sistema di conservazione e del servizio per la tenuta del protocollo informatico, e il comma 1-ter, che stabilisce a livello di norma generale quanto già indicato nella normativa tecnica del 2004 in materia di affidamento della funzione conservativa “ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche”.

La novità principale del CAD in questo ambito è tuttavia costituita soprattutto dall’articolo 44-bis (conservatori accreditati), che stabilisce un duplice livello di qualità del servizio prevedendo la possibilità di richiedere l’accredimento presso DigitPA per “i soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza” (comma 1).

I dettagli tecnici, tutt’altro che secondari anche se non esaurienti, sono presenti nel comma seguente allorché si richiamano “in quanto compatibili”, gli articoli 26 (requisiti dei certificatori), 27 (certificatori qualificati), 29 (accredimento, ad eccezione del comma 3, lettera a) e 31 (vigilanza) ovvero gli obblighi e i controlli previsti dal CAD per gli enti certificatori che rilasciano certificati di firma digitale. Nel caso specifico si riconosce che tale funzione possa essere affidata anche a soggetti pubblici e che i soggetti privati (comma 3) che intendano accreditarsi debbano essere “costituiti in società di capitali con capitale sociale non inferiore a euro 200.000”. Per comprendere meglio il significato e le conseguenze operative del nuovo articolo, soprattutto in relazione alla natura e alle modalità dell’accredimento dei soggetti che conservano e della certificazione dei processi di conservazione¹¹ - sarà necessario attendere i requisiti previsti da

¹¹ Non è di per sé evidente dalla lettura del dispositivo se si tratti di due tipi di attività da affidare allo stesso soggetto o a soggetti distinti.

DigitPA per l’accredimento dei cosiddetti soggetti conservatori. La qualificazione dei soggetti conservatori ai fini dell’accredimento dovrebbe prendere in considerazione la capacità di:

- dimostrare l’affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere l’attività di conservazione;
- utilizzare personale dotato delle conoscenze specifiche, dell’esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della gestione documentale e conservazione di documenti informatici e della dimestichezza con procedure di sicurezza appropriate;
- rispettare le norme del CAD e le regole tecniche di cui all’articolo 71;
- applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;
- utilizzare sistemi affidabili e sicuri di conservazione di documenti informatici realizzati e gestiti in conformità alle disposizioni contenute nel decreto delle regole tecniche previste dal CAD e in conformità ai criteri di sicurezza dello standard ETSI e inerenti i requisiti di sicurezza dei sistemi di conservazione, ma anche in conformità ai criteri di interoperabilità dello standard UNI 11386:2010 SInCRO - Supporto all’Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali¹²;
- adottare adeguate misure contro la contraffazione dei do-

¹² Si tratta dello standard UNI 11386:2010 SInCRO - Supporto all’Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali relativo alla interoperabilità nel tempo dei dati relativi ai lotti di documenti firmati, e marcati temporalmente. Lo standard è stato approvato con il supporto di DigitPA e dell’amministrazione archivistica e con la partecipazione diretta di molti certificatori qualificati. La norma è reperibile a pagamento sul sito dell’UNI <http://webstore.uni.com/unistore/public/searchproducts>.

cumenti idonee a garantire la riservatezza, l'integrità e la sicurezza dei documenti informatici oggetto di conservazione.

È auspicabile che nei processi di valutazione l'ente incaricato del monitoraggio (DigitPA) non si limiti a eseguire verifiche solo formali o di natura esclusivamente tecnologica e coinvolga perciò esperti in ambito documentario riconoscendo il ruolo esplicito in questo campo della Direzione generale degli archivi. Oltre ai tre articoli finora esaminati, nel CAD sono presenti altre disposizioni rilevanti in materia di sicurezza e persistenza delle infrastrutture tecnologiche, che è utile qui considerare per la loro immediata connessione con i requisiti di qualità di un sistema di conservazione:

- l'articolo 50 bis (continuità operativa) prevede che “in relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongano i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività” (comma 1); che il Ministro per la pubblica amministrazione e l'innovazione assicuri l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informi con cadenza almeno annuale il Parlamento (comma 2); che le pubbliche amministrazioni definiscano (sulla base di studi di fattibilità valutati da DigitPA):
 - a. il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni; il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive; le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

- b. il piano di *disaster recovery*, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a. e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione; si prevede che DigitPA, sentito il Garante per la protezione dei dati personali, definisca le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifichi annualmente il costante aggiornamento dei piani di *disaster recovery* delle amministrazioni interessate e ne informi annualmente il Ministro per la pubblica amministrazione e l'innovazione¹³;
- l'articolo 51 (sicurezza dei dati, dei sistemi, delle infrastrutture delle pubbliche amministrazioni) stabilisce principi generali per le norme di sicurezza (definite in dettaglio nelle regole tecniche di cui all'articolo 71) con riferimento all'esigenza di rispettare criteri di esattezza, disponibilità, accessibilità, integrità e riservatezza dei dati (comma 1); stabilisce l'obbligo di DigitPA di raccordare le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici e promuovere intese con le analoghe strutture internazionali, segnalare al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche da parte delle pubbliche amministrazioni (comma 1-bis) e gli obblighi delle amministrazioni di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi (comma 2-bis).

¹³ Si tratta d'altra parte di disposizioni impegnative sia sul piano organizzativo che sul piano finanziario. Non a caso i termini di applicazione per quest'ambito sono i più ampi tra quelli indicati per il CAD (15 mesi), sempre che le difficoltà economiche di questi mesi non determinino un'ulteriore slittamento a data da destinarsi. In questo caso sarebbe molto difficile per i ministri competenti imporre alle amministrazioni interventi di digitalizzazione massiva che – privi dei controlli e delle garanzie tecniche e organizzative metterebbero in pericolo la qualità e l'affidabilità delle nuove memorie digitali.

In conclusione il nuovo CAD presenta importanti e positive novità nel campo specifico della conservazione digitale, anche se molte scelte sono rinviate (ma non poteva essere altrimenti) alla successiva regolamentazione tecnica. Sono numerose le disposizioni che finalmente riconoscono la necessità di scelte di integrazione tra i processi di formazione dei documenti e quelli relativi alla loro tenuta e custodia:

- il riconoscimento della necessità di discipline particolari (da approvare con decreti *ad hoc*) per la conservazione sostitutiva di particolari tipologie di documenti analogici originali è un passo significativo che sottolinea – sia pure in un caso specifico – la necessità di intervenire precocemente nel processo di formazione dei documenti e di sviluppare strumenti basati sulla conoscenza specifica dei diversi sistemi di produzione (articolo 22 comma 3-ter)¹⁴;
- l’ancoraggio al protocollo informatico delle caselle di posta elettronica certificata attesta la centralità di un sistema unitario e organico di gestione che utilizza strumenti propri di natura archivistica (articolo 40-bis)¹⁵;
- lo stretto collegamento tra il responsabile del servizio di protocollo e archivio e il responsabile della conservazione (già ricordato in precedenza) è garanzia di continuità tecnico-documentaria nella catena delle responsabilità (articolo 44 comma 2-bis);

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

¹⁵ “Art. 40-bis. – (Protocollo informatico). - 1. Formano comunque oggetto di registrazione di protocollo ai sensi dell’articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica di cui agli articoli 47, comma 3, 54, comma 2-ter e 57-bis, comma 1”.

- le norme sull’obbligo dei piani di continuità operativa e di disaster recovery e di sicurezza costituiscono le garanzie tecnico-organizzative per la necessaria protezione dei contenuti digitali (articoli 50-bis e 51).

3.3 La nuova regolamentazione tecnica sulla conservazione

Molteplici sono i nodi che devono essere sciolti dalle regole tecniche, tra cui in particolare i livelli di responsabilità, le forme organizzative e le modalità di cooperazione tra responsabili degli archivi correnti e della conservazione digitale; la natura e i contenuti delle *policy* a supporto del processo di conservazione, che il legislatore ha individuato con la denominazione di manuale di conservazione; i principi e i modelli per sviluppare l’interoperabilità nella trasmissione dei documenti e nel trasferimento/versamento di archivi.

La norma di maggior rilievo rispetto all’esame qui affrontato è naturalmente il provvedimento specifico sulla conservazione ai sensi degli articoli 44 e 44-bis del CAD che abroga la deliberazione Cnipa 11/2004 e ridefinisce sostanzialmente l’intero sistema di conservazione costituito dall’insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti e degli altri oggetti in esso contenuti (ad esempio i metadati e le informazioni relative ai pacchetti di archiviazione, versamento e distribuzione). Le regole pubblicate sul sito di DigitPA nella forma di bozze presentano un quadro coerente e innovativo che qui si presenta in sintesi sottolineando che si tratta ancora di un testo preliminare, anche se ben articolato e approfonditamente discusso da un gruppo di lavoro cui hanno partecipato tra gli altri i rappresentanti delle Regioni e dei Ministeri competenti, la Direzione generale degli archivi, il coordinatore del Comitato UNI per la gestione dei documenti.

Coerentemente con il modello OAIS che le regole hanno adottato come riferimento logico e architettura generale, gli ogget-

ti della conservazione sono organizzati a fini di trasferimento, tenuta nel deposito e consultazione in pacchetti informativi (di versamento, archiviazione e distribuzione). Nel caso dei pacchetti di archiviazione si definiscono (negli allegati alle regole) specifiche della struttura dei dati in grado di assicurare la reciproca interoperabilità e si fa esplicito riferimento allo standard UNI SInCRO che era stato sviluppato proprio con l'obiettivo di superare i limiti concettuali e strutturali della delibera 11/2004.

Specificata attenzione è poi dedicata ai modelli organizzativi: innanzi tutto si stabilisce la chiara distinzione tra le fasi di gestione e quelle di conservazione e, ai sensi dell'articolo 44 comma 1-ter del CAD, si precisa che la conservazione può essere svolta sia internamente al soggetto produttore che affidandola anche parzialmente ad altri soggetti pubblici o privati in grado di offrire adeguate garanzie organizzative e tecnologiche. Si prevede che le pubbliche amministrazioni – qualora affidino il servizio all'esterno – debbano necessariamente fare riferimento a conservatori accreditati pubblici o privati. Si definiscono i ruoli del processo di conservazione: produttore (che nelle pubbliche amministrazioni corrisponde al responsabile del servizio per la tenuta del protocollo informatico), utente e responsabile della conservazione. L'articolo 6 stabilisce le modalità di gestione dei diversi livelli di responsabilità e, comunque, prescrive che le modalità operative di trasferimento dei pacchetti di versamento siano descritte nel manuale di conservazione e che si definiscano accordi formali tra i diversi attori del processo. Si chiariscono in particolare i compiti del responsabile della conservazione (cui si attribuisce la funzione generale di definire e attuare le politiche complessive del sistema di conservazione e governarne la gestione in relazione al modello organizzativo), le modalità di definizione e limitazione della delega che deve essere formalizzata e motivata e, in caso di affidamento a terzi, deve essere gestita con “un contratto/convenzione di servizio che preveda

l'obbligo del rispetto del manuale di conservazione predisposto dal responsabile della conservazione”. In sostanza si riduce la discrezionalità degli interventi e si accrescono notevolmente gli obblighi di trasparenza al fine di accrescere gli strumenti di verifica e le garanzie di auditing accurati.

In particolare al responsabile della conservazione sono riconosciuti compiti alquanto impegnativi (articolo 7):

- a. definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare;
- b. gestire il processo di conservazione garantendone nel tempo la conformità alla normativa vigente;
- c. generare il rapporto di versamento, secondo le modalità previste dal manuale;
- d. generare e sottoscrivere il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e. effettuare il monitoraggio della corretta funzionalità del sistema di conservazione;
- f. assicurare la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;
- g. adottare misure per verificare e prevenire il degrado dei sistemi di memorizzazione e delle registrazioni, l'obsolescenza dei formati al fine di garantire la conservazione e l'accesso ai documenti informatici;
- h. provvedere alla duplicazione o copia dei documenti informatici all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- i. adottare le misure necessarie per la sicurezza fisica e logica del sistema di conservazione;

- j. richiedere la presenza di un pubblico ufficiale, nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- k. assicurare l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza ai diversi organismi competenti previsti dalle norme vigenti;
- l. provvedere, nel caso di amministrazioni statali, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;
- m. predisporre il manuale di conservazione e curarne l'aggiornamento periodico e in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

In relazione a quanto previsto dall'articolo 44, comma 1-ter del CAD, il responsabile della conservazione può richiedere di certificare la conformità del processo di conservazione ad altri soggetti, pubblici o privati, eventualmente accreditati presso DigitPA come certificatori del sistema di conservazione ai sensi dell'articolo 44-bis, comma 1 dello stesso Codice. Con tale indicazione le regole interpretano il dettato della legge distinguendo le responsabilità per l'accreditamento e quelle per la certificazione e, allo stesso tempo, riconoscendo che i soggetti accreditati sono titolati a certificare i processi di conservazione.

In tema di titolarità della funzione i commi 3 e 4 dell'articolo 7 stabiliscono che nelle pubbliche amministrazioni il ruolo del responsabile della conservazione sia svolto da un dirigente o da un funzionario delegato formalmente designato e che tale ruolo possa essere assegnato al responsabile del servizio per la gestione dei documenti.

L'articolo 8 propone uno schema di massima del manuale di conservazione. In sintesi il manuale descrive "l'organizzazio-

ne, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione".

Infine l'articolo 9 tratta l'articolazione del processo di conservazione che include le fasi seguenti:

- l'acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico;
- la verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione;
- il rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla lettera b. abbiano evidenziato delle anomalie;
- la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;
- l'eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal responsabile della conservazione, ove previsto nel manuale di conservazione;
- la preparazione e la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nel pacchetto di archiviazione (definito in allegato alle regole) e secondo le modalità riportate nel manuale della conservazione;

- la preparazione e la sottoscrizione con la firma digitale o firma elettronica qualificata, ove previsto nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione sulla base della richiesta dell'utente;
- la produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione al fine di garantire l'interoperabilità tra sistemi di conservazione;
- la produzione dei duplicati informatici o delle copie informatiche effettuati per richiesta degli utenti;
- l'eliminazione dal sistema di conservazione del pacchetto di archiviazione alla decorrenza dei termini previsti dalla norma dandone informativa al produttore secondo quanto previsto dalla normativa vigente, che, nel caso degli archivi pubblici o archivi privati, che rivestono interesse storico particolarmente importante, implica anche la previa autorizzazione allo scarto da parte del Ministero per i beni e le attività culturali.

Si prevede infine che nel caso dei sistemi di conservazione delle pubbliche amministrazioni e dei sistemi di conservazione dei conservatori accreditati, ai fini della vigilanza da parte di DigitPA su questi ultimi, i dati e/o le copie di sicurezza siano conservati sul territorio nazionale e sia garantito l'accesso presso la sede del produttore.

Le novità sono quindi numerose e largamente positive: la flessibilità è rispettata senza ledere (anzi assicurando) le esigenze di interoperabilità; si privilegia la dimensione di responsabilità dei soggetti e si definiscono soprattutto requisiti metodologici e di natura organizzativa, demandando a documenti *ad hoc* (opportunamente strutturati come nel caso del manuale di conservazione) le scelte tecniche specifiche.

Nonostante le scelte importanti e positive operate dal legislatore in questi ultimi mesi, la normativa nazionale non risolve

completamente tutti i difficili problemi e le numerose sfide della sedimentazione archivistica digitale. Si limita, necessariamente, a stabilire parametri generali sulla validità del documento, a definire responsabilità e a delineare modelli organizzativi distinti per il settore pubblico e per quello privato. In altra sede dovranno essere approfondite e definite le questioni altrettanto cruciali della tutela dei nuovi beni digitali prodotti, ad esempio in relazione alla tempistica della consegna al custode fidato nel caso degli archivi storici prodotti dalla pubblica amministrazione e alle nuove forme di organizzazione dei poli digitali di conservazione che si vanno costituendo a livello nazionale presso le Regioni o presso altre istituzioni di natura pubblica e privata. Si dovrà, tra l'altro, affrontare con molta oculatezza il problema dei versamenti precoci, della loro periodicità e dei modi operativi per garantire che le aggregazioni archivistiche mantengono la coerenza originaria. Anche l'attività descrittiva e i modi per rendere consultabili i patrimoni documentari digitali dovranno essere oggetto di ulteriore riflessione, tenendo conto delle concrete esperienze avviate.

Si tratta tuttavia di questioni che potranno trovare risposte adeguate nella sperimentazione ed essere sostenute dalla ricerca interdisciplinare, a condizione che il quadro normativo qui anticipato trovi conferma nelle fasi successive del suo iter di approvazione e che il nuovo spirito di collaborazione tra discipline, amministrazioni e settori operativi, di cui questi provvedimenti sono positiva testimonianza, continui a guidare il lavoro delle istituzioni cui è affidato il compito impegnativo di garantire il futuro delle memorie digitali.

Stefano Pigliapoco

Protocollare e archiviare la PEC e altri documenti informatici

Stefano Pigliapoco

Docente di Informatica documentale e multimediale presso l'Università degli Studi di Macerata. La sua attività di studio e ricerca riguarda il documento informatico, la comunicazione digitale, la dematerializzazione della documentazione amministrativa, il reengineering dei processi, la formazione, gestione e conservazione di archivi digitali in ambito pubblico e privato. È componente di diversi comitati scientifici e gruppi di ricerca sulla digital preservation.

La relazione analizza le peculiarità dei messaggi di Posta Elettronica Certificata e fornisce alcune indicazioni su come protocolarli e archivarli.

1. Una premessa necessaria

La pubblica amministrazione, essendo preposta alla gestione del bene comune, è tenuta a motivare le sue decisioni e a dare evidenza delle attività che svolge, dimostrandone la correttezza e la legittimità. Ad essa si applicano i principi di trasparenza, pubblicità e consultabilità, da cui discende l'obbligo di far conoscere l'azione amministrativa e gli aspetti dell'organizzazione.

La stessa definizione di procedimento amministrativo, che lo indica come “serie di atti e operazioni funzionalmente collegate in relazione ad un unico effetto”¹, rileva per esso il principio di documentalità, per cui ogni passaggio dalla fase dell'iniziativa a quella della deliberazione e lo stesso provvedimento finale devono possedere l'evidenza documentale.

L'esigenza di avere memoria delle attività svolte e di poterne

¹ Adunanza plenaria del Consiglio di Stato del 28/01/1961.

dimostrare la regolare esecuzione attraverso l'esibizione della relativa documentazione spinge le organizzazioni pubbliche a formare i fascicoli archivistici, intesi come "insieme ordinato dei documenti acquisiti o prodotti durante lo svolgimento di un procedimento amministrativo, di un'attività o un progetto, oppure riguardanti una persona fisica o giuridica". Tali fascicoli nascono negli uffici cui competono le relative attività, ma poi convergono nell'archivio dell'ente, dove sono conservati per il tempo necessario.

I vincoli cui sono soggette le pubbliche amministrazioni per la tenuta e la conservazione dei loro archivi, sono chiaramente esposti nel Dlgs. 22 gennaio 2004, n. 42, recante il Codice dei beni culturali e del paesaggio:

- l'art. 10 dichiara che gli archivi e i singoli documenti dello Stato, delle regioni, degli enti pubblici territoriali, nonché di ogni altro ente o istituto pubblico, sono beni culturali e quindi soggetti alle disposizioni in materia di tutela e valorizzazione;
- l'art. 30 impone allo Stato, alle regioni, agli altri enti pubblici territoriali nonché ad ogni altro ente o istituto pubblico, l'obbligo di garantire la sicurezza e la conservazione dei beni culturali di loro appartenenza, nonché di conservare i propri archivi nella loro organicità e di ordinarli;
- l'art. 53 afferma che i beni culturali appartenenti allo Stato, alle regioni e agli altri enti pubblici territoriali costituiscono il demanio culturale e quindi sono inalienabili.

La transizione dal documento cartaceo al documento informatico, che determina la trasformazione dell'archivio cartaceo in archivio digitale o ibrido, non introduce modifiche alle disposizioni sopra richiamate, le quali, pertanto, devono essere attuate anche dalle cosiddette "amministrazioni pubbliche digitali".

In altri termini, dalla lettura combinata del Codice dell'amministrazione digitale, contenuto nel Dlgs. 8 marzo 2005, n. 82, recentemente modificato con il Dlgs. 30 dicembre 2010, n. 235, e del Codice dei beni culturali e del paesaggio, si rileva per le pubbliche amministrazioni l'obbligo di garantire sia la produzione, ricezione, trasmissione e gestione dei documenti informatici, anche sottoscritti con firma elettronica, sia la formazione e la conservazione degli archivi digitali o ibridi.

2. La Posta Elettronica Certificata

L'art. 1, c. 1, lett. g), del DPR n. 68/2005, recante disposizioni per l'utilizzo della Posta Elettronica Certificata, definisce Posta Elettronica Certificata "ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici". Si tratta di un sistema di comunicazione elettronica introdotto dal legislatore italiano con l'obiettivo di fornire alle pubbliche amministrazioni, ai cittadini, ai professionisti e alle imprese uno strumento affidabile per trasmettere e ricevere contenuti digitali con garanzia di recapito, riservatezza, integrità e provenienza.

La garanzia della provenienza di un'email certificata, ossia l'identificazione del titolare della casella da cui proviene un messaggio di PEC², discende da tre caratteristiche del servizio:

- a. il soggetto che trasmette il messaggio, all'atto della connessione al punto di accesso, viene identificato - con ragionevole sicurezza - dal suo gestore tramite le credenziali (userid e password) che gli ha rilasciato insieme alla casella;

² Il titolare di una casella di Posta Elettronica Certificata di cui al DPR n. 68/2005 può essere una persona fisica o giuridica, una pubblica amministrazione o qualsiasi ente, associazione o organismo, mentre il titolare di una casella certificata del cittadino (servizio Postacertificat@ di cui al DPCM 6 maggio 2009) può essere solo una persona fisica.

- b. il canale di comunicazione tra mittente e destinatario implementa meccanismi tecnici tali da garantire la sicurezza e la riservatezza di tutte le connessioni: tra mittente e punto di accesso, tra gestore e gestore, tra punto di consegna e destinatario;
- c. i gestori del servizio di PEC tengono traccia, per almeno trenta mesi, in un registro informatico denominato “log dei messaggi”, delle operazioni effettuate per la trasmissione delle email certificate. E tale registro è conservato con modalità tali da assicurare la riservatezza, sicurezza, integrità ed inalterabilità nel tempo delle informazioni in esso contenute.

Allo stato attuale, per effetto della normativa vigente, accanto ai canali tradizionali della posta cartacea e degli apparecchi fax, nelle pubbliche amministrazioni è operativo il canale della Posta Elettronica Certificata che, al pari degli altri mezzi di comunicazione, può essere utilizzato da cittadini, professionisti, imprese o altri enti pubblici, per inoltrare messaggi rilevanti ai fini amministrativi.

3. Rilevanza giuridica dei messaggi di PEC

Il Codice dell'amministrazione digitale riconosce piena efficacia alle trasmissioni di documenti informatici eseguite con una casella di PEC:

- l'art. 45, c. 1, dichiara che “i documenti trasmessi da chiunque a una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale”;
- l'art. 47, c. 1, sottolinea che le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica e sono valide ai fini

del procedimento amministrativo una volta che ne sia verificata la provenienza;

- l'art. 47, c. 2, precisa che “ai fini della verifica della provenienza, le comunicazioni sono valide se: 1) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata; 2) ovvero sono dotate di protocollo informatizzato; 3) ovvero è comunque possibile accertarne altrimenti la provenienza secondo quanto previsto dalla normativa vigente; 4) ovvero sono trasmesse attraverso sistemi di Posta Elettronica Certificata di cui al DPR n. 68/2005”;
- l'art. 65, c. 1, lett. c-bis), considera valide le istanze e le dichiarazioni presentate alle pubbliche amministrazioni dall'autore per via telematica mediante la propria casella di PEC, purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato³.

Queste disposizioni sono sufficienti a tracciare il profilo giuridico dei messaggi di PEC. Essi soddisfano il requisito della forma scritta, possono rappresentare un'istanza o una dichiarazione presentata a una pubblica amministrazione per via telematica, equivalgono a documenti informatici sottoscritti con firma elettronica⁴ e costituiscono comunicazione valida ai fini del procedimento amministrativo.

³ Qui il legislatore pone l'accento sull'esigenza di associare le caselle di PEC ai rispettivi titolari in modo che sia possibile attribuire ad essi la paternità dei messaggi inoltrati.

⁴ Si segnala che nella bozza delle nuove regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, firme elettroniche qualificate, firme elettroniche digitali e validazione temporale dei documenti informatici, recentemente pubblicata sul sito di DigitPA, l'invio tramite Posta Elettronica Certificata di cui all'art. 65, comma 1, lettera c-bis), del CAD, effettuato richiedendo la ricevuta completa di cui all'art. 1, comma 1, lettera i) del decreto 2 novembre 2005, recante le regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della Posta Elettronica Certificata, costituisce, nei confronti della pubblica amministrazione, firma elettronica avanzata del messaggio spedito.

4. Protocollo dei messaggi di PEC

Il legislatore, anche se non era necessario perché l'art. 53 del DPR 28 dicembre 2000, n. 445, recante il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, indica chiaramente che sono soggetti a registrazione tutti i documenti informatici delle pubbliche amministrazioni, nell'art. 40-bis, c. 1, del Codice dell'amministrazione digitale (CAD), ha confermato l'obbligo della registrazione di protocollo per:

- le comunicazioni che pervengono o sono inviate attraverso la casella di PEC istituzionale e gli altri eventuali indirizzi di posta elettronica dichiarati all'Indice degli indirizzi delle amministrazioni pubbliche (www.indicepa.gov.it);
- i messaggi ricevuti o trasmessi attraverso l'indirizzo di PEC pubblicato sul sito istituzionale dell'amministrazione per accogliere le richieste dei cittadini;
- i documenti scambiati tra le pubbliche amministrazioni per posta elettronica o in cooperazione applicativa;
- le istanze e le dichiarazioni presentate per via telematica con le modalità di cui all'articolo 65, c. 1, lett. c-bis).

I messaggi di PEC che rientrano nell'azione di una pubblica amministrazione devono essere non solo protocollati, ma anche classificati, inseriti nei rispettivi fascicoli elettronici e conservati nell'archivio digitale⁵. Per eseguire tutte queste operazioni, le pubbliche amministrazioni devono implementare sistemi tecnologicamente avanzati per la gestione informatica dei documenti e adottare modelli organizzativi e archivistici compatibili con

⁵ Ai sensi dell'art. 42, c. 2, del CAD, la pubblica amministrazione titolare del procedimento amministrativo deve raccogliere in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati, dando comunicazione per via telematica dell'avvio del procedimento come stabilito dall'articolo 10 della legge 7 agosto 1990, n. 241.

le peculiarità dei documenti informatici e dell'archivio digitale.

In primo luogo, devono evitare l'eccessiva proliferazione degli indirizzi di PEC dichiarati all'Indice degli indirizzi delle amministrazioni pubbliche (www.indicepa.gov.it) e/o pubblicati sul loro sito istituzionale.

L'attivazione di una casella di posta certificata e la sua pubblicazione sull'Indice degli indirizzi delle amministrazioni pubbliche e/o sul sito istituzionale dell'ente abilitano soggetti esterni a utilizzarla per presentare istanze e dichiarazioni per via telematica. Pertanto, queste caselle devono essere costantemente monitorate per gestire prontamente i documenti informatici in arrivo e rispettare i tempi fissati per lo svolgimento dei procedimenti amministrativi. E ciò appare tanto più difficile quanto più elevato è il numero degli indirizzi di PEC dichiarati e assegnati ai vari uffici, dirigenti e responsabili di procedimento.

Inoltre, tanto maggiore è il numero delle caselle di PEC attivate, tanto più grande è il rischio che i messaggi finiscano per essere memorizzati nei sistemi sui quali sono ricevuti o prodotti, con conseguente dispersione dei documenti informatici, che rende difficile, se non addirittura impossibile, la formazione di fascicoli elettronici completi.

In secondo luogo, le pubbliche amministrazioni devono connettere direttamente le caselle di PEC istituzionali al sistema di gestione informatica dei documenti di cui al DPR n. 445/2000 (protocollo informatico).

L'integrazione funzionale tra il servizio di Posta Elettronica Certificata e il sistema di gestione informatica dei documenti permette di acquisire i messaggi in entrata direttamente sul sistema di protocollo informatico e di utilizzare lo stesso sistema per formare automaticamente quelli in uscita, allegandovi i documenti registrati con le relative segnature di protocollo. In questo modo,

si evita la dispersione dei messaggi di PEC in tanti sistemi e si spinge il personale alla loro protocollazione e archiviazione prima della trattazione da parte degli uffici competenti, o prima della loro spedizione ai destinatari.

Inoltre, la capacità del sistema di gestione informatica dei documenti di formare automaticamente i messaggi di PEC in uscita permette di decentrare le operazioni di protocollazione e spedizione dei documenti nelle unità organizzative di competenza, senza essere costretti ad attivare un numero troppo elevato di caselle di posta certificata.

Verso l'integrazione funzionale tra il sistema di gestione informatica dei documenti e il servizio di Posta Elettronica Certificata indirizza anche la Circolare 19 aprile 2010, n. 2, del Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei Ministri, nella quale si rileva la necessità di "convogliare il flusso delle email relativo alle caselle di PEC sullo stesso sistema di protocollazione utilizzato per i documenti tradizionali" e l'opportunità di "adottare prodotti di gestione del protocollo informatico predisposti per il trattamento dei messaggi e degli allegati veicolati via PEC, o soluzioni in grado di "collegare" il sistema di gestione della posta elettronica di tipo PEC e quello di gestione del protocollo". Per motivi analoghi, nella stessa circolare, si raccomanda di "adottare sistemi di gestione documentale che consentano la gestione integrata e la tenuta dei messaggi, degli allegati e delle ricevute nell'ambito della gestione del fascicolo informatico".

Le pubbliche amministrazioni, o in alternativa DigitPA a livello nazionale, dovrebbero elaborare delle linee guida per la corretta formazione dei messaggi di Posta Elettronica Certificata che veicolano istanze e dichiarazioni valide ai fini dei procedimenti amministrativi.

La posta elettronica è uno strumento di comunicazione che ha raggiunto una diffusione mondiale e che oggi un pò tutti utilizziamo sia in ambito lavorativo, sia a livello personale. Con l'introduzione del servizio di Posta Elettronica Certificata, i messaggi trasmessi a una pubblica amministrazione diventano istanze e dichiarazioni valide ai fini del procedimento amministrativo, per cui devono essere formati adottando le stesse regole previste per i documenti informatici.

Innanzitutto, non devono contenere macroistruzioni o codice eseguibile, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati in esso rappresentati⁶. Ad esempio, se una pubblica amministrazione ricevesse un messaggio di PEC al cui interno è presente il link a un file memorizzato sul sito web del mittente, si troverebbe nella condizione di dover protocollare e archiviare un documento il cui contenuto può essere cambiato in qualsiasi momento, semplicemente modificando sul sito web l'oggetto digitale collegato.

Secondariamente, i documenti informatici, anche sottoscritti con firma digitale, allegati a un messaggio di PEC devono essere prodotti in un formato elettronico compatibile con il processo di conservazione digitale, cioè un formato elettronico di tipo aperto, standard, documentato e indipendente dalle piattaforme tecnologiche utilizzate per la loro rappresentazione.

Queste considerazioni evidenziano la necessità di fornire ai cittadini, ai professionisti, alle imprese e al personale delle pubbliche amministrazioni le istruzioni per la corretta formazione dei messaggi di Posta Elettronica Certificata, in modo da ricevere, produrre e archiviare documenti informatici ben formati e conservabili in forma digitale.

⁶ Si veda l'art. 3, c. 3, del DPCM 30 marzo 2009, recante le regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.

Il sistema di gestione informatica dei documenti utilizzato da una pubblica amministrazione deve essere dotato di funzionalità *ad hoc* per la trattazione dei messaggi di PEC.

Un messaggio di Posta Elettronica Certificata è un oggetto digitale composto da più parti: il testo del messaggio, i dati di certificazione che identificano il titolare della casella di provenienza, gli eventuali file allegati che possono anche essere sottoscritti con firma digitale, altri dati tecnici propri della comunicazione per via telematica. Pertanto, per protocollare correttamente un messaggio di PEC è necessario un sistema che presenti all'operatore del protocollo le parti che lo compongono e gli permetta di selezionare e di descrivere prima il documento principale - che può essere rappresentato dal testo del messaggio o da un file allegato all'email - e poi gli eventuali allegati al documento.

Benedetto Santacroce

Dalla firma digitale alla firma biometrica: quadro giuridico di riferimento per l'applicazione dei nuovi dispositivi di firma

Benedetto Santacroce

Benedetto Santacroce è Professore presso l'Università Marconi di Roma, avvocato tributarista e rappresentante del Consiglio nazionale dei Dottori Commercialisti presso la FEE Federation des Experts comptables européens a Bruxelles. È stato esperto nazionale distaccato presso la Commissione Europea direzione generale fiscalità e Unione doganale, ha collaborato con il Ministero del Lavoro per la rendicontazione e gli obblighi fiscali connessi ai tributi erogati nell'ambito del FSE. Pubblicista, la sua firma appare su numerose riviste e giornali specializzati in materia fiscale e doganale, tra cui "Il Sole 24 Ore". È autore di vari libri in materia di trattamento dei documenti fiscali e del lavoro.

Le modifiche apportate dal Dlgs. 235/2010 al CAD - Codice dell'amministrazione digitale - rispondono all'esigenza di adeguare il testo normativo all'evoluzione tecnologica intervenuta garantendo allo stesso tempo una maggiore flessibilità operativa degli strumenti utilizzati. Per questa ragione il Legislatore ha introdotto il principio della neutralità tecnologica anche con riguardo al documento informatico, con la finalità di ridurre al massimo le restrizioni alle modalità di formazione dei documenti promuovendo altresì l'interoperabilità dei sistemi.

Da ciò deriva il riconoscimento della validità di tutti gli standard tecnici presenti sul mercato. Si tratta della stessa via tracciata dall'Unione Europea con la Direttiva 2010/45/Ue del 13 luglio 2010 in materia di fatturazione IVA, il cui recepimento è stato di recente oggetto di delega al Governo con il disegno di legge Comunitaria 2011.

Sono state di fatto semplificate le regole di emissione delle fatture elettroniche con libertà per i soggetti passivi di struttura-

re controlli interni di gestione idonei ad assicurare l'autenticità dell'origine e l'integrità del contenuto documentale. Sinora tali requisiti potevano essere garantiti solamente attraverso l'apposizione di firma digitale o l'utilizzo di trasmissioni EDI, strumenti questi di cui comunque ci si può continuare ad avvalere.

Il riconoscimento della piena validità giuridica di documenti informatici sottoscritti con soluzioni di firma elettronica avanzata risponde proprio al principio di neutralità tecnologica. Di fatto, il documento informatico, le sue copie e duplicati hanno una efficacia probatoria graduata in base alla tipologia di firma elettronica che gli viene apposta dall'autore o dal gestore, cioè dalla persona fisica o giuridica responsabile della tenuta del documento stesso.

In questa logica, anche l'ampliamento di alcuni processi alla firma elettronica avanzata, accanto alla firma elettronica digitale qualificata, come vedremo analizzando il Decreto approvato da DigitPA il 4 luglio scorso, offre delle opportunità agli operatori di rendere più flessibili la gestione e la conclusione di specifiche operazioni commerciali.

1. Valore probatorio

Le regole tecniche predisposte da DigitPA, pubblicate in consultazione il 4 luglio (firma elettronica avanzata) e 5 agosto 2011 (documento informatico e conservazione sostitutiva), seguono la strada tracciata dal CAD. Il documento informatico non sottoscritto digitalmente è, secondo l'articolo 20, comma 1-bis del CAD, liberamente valutabile in giudizio in base al principio di neutralità tecnologica.

Il suo valore probatorio e l'idoneità a soddisfare il requisito della forma scritta dipendono quindi dalle caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità che il sistema tecnologico utilizzato è in grado di garantire.

Tuttavia il documento informatico, quando sottoscritto con firma elettronica qualificata o digitale oppure anche con firma elettronica avanzata, acquista di per sé un'efficacia probatoria pari a quella della scrittura privata ai sensi dell'articolo 2702 del codice civile.

Costituisce quindi piena prova sino a querela di falso della provenienza delle dichiarazioni di chi l'ha sottoscritto. Solamente per gli atti di costituzione e trasferimento dei diritti reali immobiliari di cui all'articolo 1350 del codice civile viene richiesta obbligatoriamente la sottoscrizione, a pena di nullità, con firma qualificata o digitale.

Ulteriori semplificazioni per le copie, analogiche ed informatiche, e per i duplicati di un documento informatico cui è riconosciuto il medesimo valore probatorio dell'originale informatico da cui sono tratti.

Il documento informatico può quindi essere sottoscritto anche con l'utilizzo di soluzioni di firma elettronica avanzata: dal combinato disposto del CAD e delle regole tecniche di generazione, apposizione e verifica delle firme elettroniche, in consultazione, emerge un quadro normativo che favorisce e persegue lo sviluppo di strumenti in grado di semplificare l'uso delle nuove tecnologie.

L'obiettivo finale è quello di garantire una sostanziale e piena equiparazione del documento informatico con quello cartaceo, passando attraverso un incremento delle tipologie di firme elettroniche utilizzabili ai fini della redazione.

Quindi, con valenza probatoria modulata in ragione della firma utilizzata, alle preesistenti firma elettronica, firma elettronica qualificata e firma digitale, è stata affiancata la firma elettronica avanzata recependo integralmente la normativa europea contenuta nella Direttiva del Parlamento europeo e del Consiglio n.

1999/93/CE. Le regole tecniche predisposte da DigitPA sulle firme elettroniche, riconoscono la possibilità di realizzare, in forma libera, soluzioni di firma elettronica avanzata, senza necessità di alcuna autorizzazione preventiva ma con il rispetto di una serie di requisiti minimi.

Si sono così liberalizzate le tipologie di firme avanzate, non vincolandole più ad un certificato qualificato o ad un dispositivo sicuro come invece richiesto per le firme qualificate e per quelle digitali, entrambe *species* del genere firma avanzata. Per una valida sottoscrizione è infatti sufficiente che il soggetto firmatario continui ad avere un controllo esclusivo sui mezzi che gli permettono di firmare un documento.

Le stesse regole tecniche fanno non a caso riferimento a soluzioni di firma avanzata, lasciando così agli operatori massima autonomia nell'individuazione delle modalità ritenute più idonee ad apporre una valida sottoscrizione all'interno di un più generale e complesso processo non solo tecnologico ma anche contrattuale.

Nel dettaglio, le firme elettroniche sono classificabili nei due generi della firma elettronica e della firma elettronica avanzata. La firma elettronica consiste solamente in un metodo di identificazione informatica realizzato attraverso l'insieme di dati in forma elettronica, allegati o connessi tramite associazione logica ad altri dati elettronici.

Di fatto, utilizziamo la firma elettronica oramai quotidianamente, senza neppure averne la consapevolezza, quando ad esempio digitiamo il codice PIN allo sportello bancomat, oppure quando ci vengono richieste credenziali, quali l'identificativo utente e la password, per accedere alle caselle di posta elettronica.

La firma elettronica si associa solamente al documento cui è apposta, restando pur sempre un elemento distinto da questo. Al contrario l'insieme di dati che caratterizza la firma elettronica

avanzata consente non solo l'identificazione del firmatario del documento ma garantisce anche la loro connessione univoca al firmatario, in quanto creati con mezzi sui quali tale soggetto conserva un controllo esclusivo.

Il collegamento ai dati sottoscritti con la firma è infatti tale da consentire di rilevare se i dati stessi sono stati successivamente modificati. In altri termini, a differenza della firma elettronica semplice, quella qualificata realizza un'unione inscindibile tra documento informatico e sua sottoscrizione.

La firma elettronica qualificata si declina a sua volta nelle due *species* della firma elettronica qualificata e della firma digitale. La firma qualificata è infatti una firma avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.

La firma digitale, invece, è un particolare tipo di firma elettronica avanzata basato su un sistema di due chiavi crittografiche, una pubblica e l'altra privata.

2. Soluzioni di firma elettronica avanzata

La firma elettronica avanzata, a differenza di quella qualificata e di quella digitale, non necessita né di un certificato qualificato né di un dispositivo sicuro per la sua valida apposizione.

La definizione del CAD opera infatti solamente un generico riferimento ai mezzi di cui il firmatario dispone e su cui esercita un controllo esclusivo.

Le nuove regole tecniche, ad oggi in consultazione e che, una volta adottate, andranno a sostituire quelle approvate con DPCM 30 marzo 2009, dettano le modalità di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.

Le regole sulle firme avanzate, contenute nel titolo V, si caratterizzano per la libertà riconosciuta ai soggetti erogatori di in-

dividuare soluzioni di firma idonee senza necessità di alcuna autorizzazione preventiva. L'unico limite introdotto alla firma elettronica avanzata, quando realizzata secondo le regole tecniche, consiste nella sua utilizzabilità esclusivamente nei rapporti giuridici intercorrenti tra il sottoscrittore ed il soggetto che ha realizzato per proprio conto la soluzione di firma, oppure si è avvalso di quelle di terzi, al fine di utilizzarla nel processo di dematerializzazione dei rapporti intrattenuti per motivi istituzionali, societari o commerciali.

Non esiste alcun vincolo tecnologico alla realizzazione di soluzioni di firma avanzata: è sufficiente il rispetto di requisiti minimi oggettivi e soggettivi.

3. Requisiti soggettivi

Oltre alle caratteristiche oggettive, le regole tecniche richiedono il rispetto di una serie di requisiti soggettivi per coloro che realizzano soluzioni di firma avanzata.

La realizzazione può essere effettuata per proprio conto, con sistemi proprietari, al fine di utilizzare le soluzioni nel processo di dematerializzazione dei rapporti intrattenuti con soggetti terzi per motivi istituzionali, societari o commerciali.

Le soluzioni possono inoltre essere realizzate anche come scopo dell'attività di impresa ai fini della fornitura a terzi, i quali le acquistano e le utilizzano a loro volta nei rapporti con la propria clientela.

Ad esclusione delle persone giuridiche pubbliche che rendono disponibili soluzioni di firma elettronica avanzata a pubbliche amministrazioni, i soggetti che realizzano per proprio conto tali soluzioni sono tenuti innanzi tutto ad identificare in modo certo l'utente, e ad informarlo dei termini e delle condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso.

L'attivazione del servizio di firma avanzata deve essere comunque subordinata alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente.

Tale dichiarazione deve inoltre essere conservata per almeno venti anni unitamente ad ogni altra informazione relativa alle caratteristiche oggettive della soluzione di firma utilizzata, garantendone la disponibilità, integrità e leggibilità e autenticità.

Eccezione in ambito sanitario, dove la dichiarazione di accettazione delle condizioni del servizio da parte dell'utente può essere effettuata anche oralmente. Inoltre dietro richiesta del firmatario, da effettuarsi con le modalità pubblicate sul proprio sito internet, si deve fornire copia della dichiarazione e delle informazioni sulla soluzione, comprese le caratteristiche delle tecnologie utilizzate.

In ogni caso, i soggetti che realizzano soluzioni proprietarie devono permettere anche l'uso della firma elettronica qualificata e della firma digitale, ove applicabile, in alternativa alla firma elettronica avanzata per i procedimenti per i quali è previsto l'uso di questa. Ciò significa che la soluzione di firma avanzata realizzata deve essere in grado di recepire la sottoscrizione della controparte apposta al documento con firma digitale o qualificata.

La soluzione deve infine prevedere un servizio di revoca della firma elettronica avanzata, ove applicabile, e un servizio di assistenza. A tutela dei firmatari e dei terzi da eventuali danni cagionati da una soluzione di firma elettronica avanzata non adeguata, i soggetti che realizzano direttamente tali soluzioni devono poter rispondere di eventuali danni derivanti dall'attività svolta per almeno seicentomila euro, anche dotandosi di una copertura assicurativa rilasciata da una società di assicurazione abilitata ad esercitare nel campo dei rischi industriali e comunicandone le modalità attraverso la loro pubblicazione anche sul proprio sito internet.

4. Caratteristiche oggettive

Nel dettaglio, la soluzione di firma avanzata per essere valida ed in linea con le regole tecniche deve garantire l'identificazione del firmatario del documento, la connessione univoca della firma al firmatario stesso ed il controllo esclusivo di questo sul sistema di generazione della firma.

Oltre a permettere l'individuazione della controparte che ha realizzato la soluzione di firma, deve essere possibile anche verificare che il documento non abbia subito modifiche dopo l'apposizione della firma.

Il firmatario deve ottenere infine evidenza di quanto sottoscritto, ad esempio attraverso la notifica di un messaggio di posta elettronica con allegato il documento firmato.

Qualunque soluzione di firma elettronica avanzata è valida purché conforme alle regole tecniche. A tal fine, verranno pubblicate apposite linee guida a cura di DigitPA proprio al fine di favorire la realizzazione di soluzioni conformi.

Tuttavia nei rapporti con la pubblica amministrazione, le regole tecniche individuano puntualmente alcune tipologie di firme elettroniche avanzate in grado di per sé di garantire la validità della soluzione adottata. Così, l'invio tramite posta elettronica certificata, effettuato richiedendo la ricevuta completa, costituisce firma elettronica avanzata del messaggio spedito. Analogamente, la Carta d'Identità Elettronica, la Carta Nazionale dei Servizi e gli altri strumenti ad esse conformi, sono utilizzabili dalle pubbliche amministrazioni per realizzare sistemi di firma avanzata.

5. Soluzione di firma biometrica

La firma biometrica può rientrare a pieno titolo tra le soluzioni di firma elettronica avanzata se il processo tecnologico nonché

contrattuale, individuato e realizzato, rispetta i requisiti soggettivi ed oggettivi richiesti dalle regole tecniche. Cnipa, ora DigitPA, ritiene da tempo come il riconoscimento biometrico della firma esamina e verifica un numero considerevole di parametri tra cui la velocità di scrittura, la pressione esercitata, l'angolo d'inclinazione della penna, l'accelerazione del movimento, il numero di volte che la penna viene sollevata dalla carta.

Si tratta di caratteristiche che permettono di ricondurre la firma apposta in maniera certa e inequivoca al soggetto sottoscrittore. L'elevato grado di accettazione da parte degli utenti abituati da sempre ad apporre la propria firma costituisce inoltre il principale vantaggio della firma biometrica.

Un utente non incontra infatti alcuna significativa differenza fra il metodo tradizionale di apposizione della firma autografa su carta e quella biometrica su una tavoletta grafica.

Prima delle nuove regole tecniche e delle modifiche al CAD, con cui è stata introdotta la firma elettronica avanzata in cui rientra la firma biometrica, quest'ultima è stata utilizzata solo come strumento per facilitare l'uso della firma digitale, in quanto ne aumenta il livello di sicurezza rispetto all'attuale grazie all'identificazione biometrica del firmatario.

Infatti l'uso di un certificato digitale, ad esempio su smart card, con le relative password non garantisce di per sé l'identificazione certa dell'interlocutore.

DigitPA, prima ancora delle regole tecniche, con nota informativa del 19 febbraio 2010 aveva comunque riconosciuto come il documento elettronico realizzato con l'uso della firma biometrica, ed associato ad un processo di firma digitale, risulta valido dal punto di vista legale ed equivalente a tutti gli effetti al documento cartaceo. Ciò sul presupposto dell'esistenza sul mercato di prodotti che integrano la firma digitale con la registrazione di

caratteristiche fisiche e dinamiche della firma autografa biometrica. Si assiste ora, anche dal punto di vista normativo, ad un'inversione di prospettiva dove la firma biometrica non affianca più e solo la firma digitale per attribuire a quest'ultima maggiore validità e sicurezza ma al contrario l'utilizzo delle tecnologie biometriche, assistito da un processo di firma digitale all'interno di un sistema strutturato anche contrattualmente, vale di per sé a riconoscere efficacia giuridica al documento elettronico così sottoscritto, equiparandolo sotto il profilo degli effetti ad un documento cartaceo.

Andrea Venturato

Dematerializzare il rapporto con i cittadini: una scelta organizzativa prima che tecnologica. Analisi progettuale

Andrea Venturato

Laureato in Ingegneria Elettronica presso l'Università degli Studi di Padova, da oltre 10 anni si occupa dello sviluppo di soluzioni innovative legate alla comunicazione digitale, alla dematerializzazione della documentazione amministrativa ed al reengineering dei processi in ambito pubblico e privato. Attualmente riveste il ruolo di Business Unit Manager.

1. Prima di partire bisogna avere le "idee" chiare

La dematerializzazione dei rapporti con il cittadino è uno degli argomenti più caldi che oggi la Pubblica Amministrazione (PA) si trova a dover affrontare nel passaggio dal mondo della carta a quello del digitale. Le tecnologie di Enterprise Content Management (ECM), che già da parecchi anni hanno un ruolo strategico negli sviluppi ICT delle aziende private, trovano oggi terreno fertile anche nella PA in quanto la recente evoluzione normativa sta favorendo sempre più l'uso di tecnologie informatiche come la firma digitale, per la produzione di documenti informatici a valore legale, e la Posta Elettronica Certificata (PEC) per l'invio sicuro degli stessi.

Un progetto per la dematerializzazione dei rapporti con il cittadino ha sicuramente notevoli impatti organizzativi in quanto introduce nuove metodologie di lavoro che vedono la progressiva eliminazione del supporto cartaceo, sostituito da quello digitale. Spesso gli aspetti tecnologici vengono considerati prioritari rispetto a quelli normativi ed organizzativi per cui il progetto prende corpo partendo dalla scelta tecnologica dell'infrastruttura su cui dovranno poggiare le applicazioni informatiche: ma come

scegliere la corretta infrastruttura applicativa se non si hanno le idee ben chiare sugli obiettivi che si vogliono raggiungere?

Serve quindi dare la priorità ad una corretta valutazione dei risultati che si vogliono raggiungere, il che non è affatto semplice, in quanto devono essere attentamente valutati alcuni aspetti strategici, che saranno descritti nel seguito, che possono rappresentare significativi spunti di riflessione per la stesura di un dettagliato piano di progetto.

- a. Analisi delle prestazioni erogate e mappatura della modulistica: è fondamentale procedere ad una dettagliata mappatura delle prestazioni che l'ente eroga a cittadini e imprese verificando sia gli aspetti procedurali e amministrativi sia la modulistica normalmente utilizzata in tutte le fasi del procedimento. La mappatura può essere suddivisa sulla base della tipologia di servizi erogati dall'ente (servizi alla persona, servizi elettorali, commercio) allo scopo di consentire una strutturazione del progetto in fasi autoconsistenti, semplificando l'introduzione delle nuove tecnologie nel processo di gestione del cambiamento. Un approfondimento su questi aspetti viene presentato nel secondo paragrafo.
- b. Individuazione della "tecnologia" che il cittadino può "facilmente" utilizzare: questo aspetto è assolutamente strategico visti gli innumerevoli strumenti di comunicazione, di differente complessità, che oggi un cittadino o un'impresa possono usare per dialogare con la PA. Un'analisi delle principali categorie di utilizzatori a cui è rivolto il servizio (professionisti, padri di famiglia, studenti), consente una precisa valutazione del livello di diffusione e di fruibilità degli strumenti tecnologici che si intendono utilizzare nella fase realizzativa, così da garantire un servizio realmente accessibile all'utente finale. Se ad esempio lo scopo è quello di consentire la presentazione di domande per l'iscrizione agli asili nido e si prevede per le

richieste telematiche la firma digitale, oggi poco diffusa tra i cittadini, il risultato sarà sicuramente un utilizzo molto limitato del servizio. Al contrario se si considera un servizio i cui interlocutori sono professionisti abilitati, come ad esempio i commercialisti, non risulta limitante richiedere nella presentazione delle domande telematiche l'utilizzo di tecnologie come la firma digitale e la posta elettronica certificata (PEC). Questo tipo di analisi, prevista per ogni singolo procedimento, se svolta in modo superficiale può rivelarsi critica e causare il mancato raggiungimento degli obiettivi del progetto (servizio inutilizzato). Purtroppo l'esperienza insegna che nei progetti di dematerializzazione il team di progetto molte volte decide a priori per l'utilizzo degli strumenti tecnologici in grado di garantire la massima certezza a livello legale e normativo, con il risultato di rendere queste iniziative di fatto scarsamente utili per migliorare la vita dei cittadini e delle imprese.

- c. Analisi dei rischi e definizione dei livelli di accettabilità (tecnologia/normativa): introdurre innovazione nei procedimenti amministrativi significa spesso doversi scontrare con nuovi strumenti tecnologici, nuove normative, scarsa giurisprudenza in materia, nuove problematiche legate alla tecnologia (es. conservazione sostitutiva e a lungo termine). Tutti questi aspetti sicuramente vanno in conflitto con il senso di sicurezza che invece garantisce l'utilizzo di soluzioni tradizionali basate sul supporto cartaceo: ciò costituisce quindi un aspetto importante nel processo di gestione del cambiamento. Spesso nella PA quando si parla di progetti innovativi di dematerializzazione l'approccio seguito è quello di richiedere una sicurezza legale e normativa superiore a quella che si è disposti ad accettare con il supporto cartaceo. Questo approccio se da un lato tende a garantire maggiormente l'amministrazione in caso di contenzioso, dall'altro riduce la fruibilità dei servizi telematici e quindi mina alla

base lo scopo di questo tipo di progetti. Un approccio sicuramente più corretto è quello di analizzare per ogni procedimento amministrativo il livello di rischio che l'ente è in grado di sopportare utilizzando strumenti tecnologici di ampia diffusione come ad esempio la semplice posta elettronica. Un approfondimento su questi aspetti viene presentato nel terzo paragrafo.

- d. Estensione del progetto: nella definizione degli obiettivi, va valutata attentamente l'estensione che si vuole dare al progetto, in quanto tale aspetto ha risvolti importanti nella scelta delle infrastrutture informatiche e applicative da utilizzare. Appare evidente che un'azienda ospedaliera che voglia dematerializzare un singolo procedimento amministrativo (richiesta di accesso agli atti) si troverà ad affrontare problematiche organizzative e tecnologiche decisamente differenti da un comune che voglia implementare uno sportello online, in grado di gestire in forma dematerializzata tutte le possibili istanze che un cittadino o un'impresa possono presentare (oltre 200). Nel caso lo scopo sia quello di creare un vero sistema di governance della macchina amministrativa è necessario prevedere che tutti i procedimenti, a prescindere dal canale di attivazione (cartaceo o digitale), siano gestiti da un univoco processo di lavorazione in grado di garantire la tracciatura delle attività svolte e l'utilizzo dei dati raccolti per la misurazione delle performance dell'amministrazione nelle sue componenti di base (servizi erogati).
- e. Analisi del processo di workflow e del livello di complessità: molto spesso nella progettazione di sistemi per la gestione informatizzata dei procedimenti amministrativi si tende a valutare nel dettaglio il funzionamento di ogni singolo procedimento producendo analisi molto voluminose (micro analisi). Questo modo di procedere presenta alcuni aspetti negativi in quanto le analisi hanno costi rilevanti, sono di

difficile implementazione pratica (visto il costo di realizzare nel sistema tutte le logiche procedurali richieste) e presentano elevata sensibilità rispetto alle variazioni organizzative. Un approccio completamente diverso prevede invece un'attività di analisi semplificata (macro analisi) in grado di portare alla realizzazione di un sistema con un unico flusso di lavoro "di alto livello": comune a tutti i procedimenti analizzati (macro processo), che garantisce un adeguato controllo del processo ma anche una buona flessibilità e resistenza alle variazioni organizzative. Un approfondimento su questi aspetti viene presentato nel quarto paragrafo.

- f. Definizione delle comunicazioni automatiche e dei canali da utilizzare: durante la fase di analisi delle prestazioni erogate una delle attività previste riguarda la mappatura delle comunicazioni obbligatorie che l'ente deve inviare al richiedente (modello di documento da utilizzare e canale di invio) in funzione del servizio richiesto. Per alcuni procedimenti sono previste a livello normativo comunicazioni legali che possono essere inviate solo tramite raccomandata o PEC, ma in molti casi può risultare sufficiente l'invio di un documento tramite posta elettronica o la pubblicazione dello stesso su un portale internet (previo consenso del richiedente). A tale scopo va analizzato per ogni prestazione l'elenco dei modelli da utilizzare (definendo il contenuto di ogni modello) e le regole di invio in funzione sia della normativa vigente che delle indicazioni espresse dal richiedente. Può risultare utile per la fase di implementazione definire una tabella riepilogativa, come quella di seguito riportata, che consenta di automatizzare il più possibile l'invio delle comunicazioni previste agevolando l'attività degli operatori e riducendo le possibilità di errore.

PRESTAZIONE: RICHIESTA ISCRIZIONE ASILO NIDO	EMAIL	PEC	SMS	LETTERA	RACCO- MANDATA	PORTALE
COMUNICAZIONE AVVIO PROCEDIMENTO	SI*		SI	SI*		SI
COMUNICAZIONE INTEGRAZIONE DOCUMENTAZIONE PRESENTATA	OP***	SI**	SI		SI**	SI
COMUNICAZIONE DI DINIEGO	OP***	SI**	SI		SI**	SI
COMUNICAZIONE DI ACCOGLIMENTO	SI*		SI	SI*		SI

(*) Lettera inviata solo nel caso il richiedente non abbia indicato l'indirizzo email

(**) Raccomandata inviata solo nel caso il richiedente non abbia indicato un indirizzo PEC.

(***) Opzionale: assieme alla raccomandata può essere inviata anche una email.

g. Misurazione delle performance (indicatori e sistemi di calcolo): introdurre nella propria organizzazione modelli di gestione, valutazione e misurazione della performance, mirati alla valorizzazione del merito, all'ottimizzazione della produttività, all'efficienza e alla trasparenza, è diventato un obiettivo strategico della Pubblica Amministrazione, a seguito delle recenti normative in materia (Dlgs. 150/09). L'analisi di progetto deve prevedere un modello di misurazione in grado di consentire, una volta identificati i KPI¹, una valutazione quantitativa del modello organizzativo adottato, allo scopo di poter eventualmente pianificare gli interventi correttivi in grado di garantire un livello di servizio sempre ottimale. Un approfondimento su questo aspetto viene presentato nel quinto paragrafo.

¹ KPI (Key Performance Indicators) è un indice che monitora l'andamento di un processo aziendale. Può essere di quattro tipi:

- indicatori generali: misurano il volume del lavoro del processo;
- indicatori di qualità: valutano la qualità dell'output di processo, in base a determinati standard
- indicatori di costo;
- indicatori di servizio, o di tempo: misurano il tempo di risposta, a partire dall'avvio del processo fino alla sua conclusione.

2. Analisi delle prestazioni erogate e mappatura della modulistica

Lo scopo di questa attività è quello di ottenere una mappatura completa dei procedimenti dell'ente rilevando per ognuno di essi le peculiarità più rilevanti (struttura competente, soggetti interni ed esterni coinvolti, tipologia utenza, particolarità, frequenza, tempistiche, normativa di riferimento, criticità, competenze tecniche, allegati, modulistica) al fine di consentire una corretta progettazione del processo di gestione. Prima di iniziare un'attività come questa è necessario predisporre tutto il materiale di indagine (schemi di rilevazione), tenendo ben distinte le analisi sulle attività di front office (sportello fisico o virtuale) da quelle di back office (servizi dedicati), raccogliendo tutte le indicazioni necessarie per preparare la modulistica (allegati obbligatori e facoltativi, cosa va chiesto e cosa va comunicato al cittadino, bollo, modalità di presentazione consentite, tag, struttura del portale online,...).

L'analisi può essere condotta creando un "Gruppo Analisi" dedicato, formato da dipendenti dei vari settori eventualmente supportati da un consulente esterno, in modo da favorire la condivisione, accrescere e valorizzare le professionalità interne e creare interesse diffuso sul progetto. I componenti del gruppo, a coppie, si incaricano di rilevare i procedimenti di settori diversi da quello di appartenenza (per evitare errori di rilevazione) prevedendo incontri periodici, ad esempio quindicinali, per mettere a fattor comune le esperienze fatte e le problematiche incontrate.

Prima di iniziare l'attività di rilevazione è necessaria una specifica formazione del Gruppo Analisi da parte di una società specializzata in questo tipo di interventi (consulenza organizzativa), allo scopo di garantire l'applicazione delle corrette tecniche di indagine, affiancando e verificando nei primi mesi l'attività degli addetti alla rilevazione. Il Gruppo Analisi si dedica sia alla rilevazione sia a una prima analisi dei procedimenti, evidenziando

le criticità e proponendo interventi migliorativi che se valutati positivamente da tutti potranno essere implementati nel nuovo sistema di gestione (miglioramento continuo). Un'attività di questo tipo ovviamente presenta delle difficoltà oggettive, di cui bisogna tenere conto nel momento in cui si va ad operare all'interno dei vari settori: spesso, infatti, ci si trova a dover fronteggiare un atteggiamento negativo da parte degli intervistati (resistenza al cambiamento).

Alcune delle difficoltà che si possono incontrare sono:

- scarsa collaborazione di alcuni responsabili;
- tendenza degli uffici a rifiutare il progetto, classificandolo come inutile aggravio di lavoro;
- difficoltà nell'ottenere indicazioni precise e non contraddittorie;
- assenza di materiale già formalizzato.

Affrontare in modo preventivo le difficoltà che i rilevatori possono incontrare è utile e a tale scopo va previsto un piano di "gestione del cambiamento" che preveda sia azioni a livello generale (presentazione del progetto, coinvolgimento dei responsabili, premi di risultato,...) sia suggerimenti sul comportamento che i rilevatori devono tenere quando incontrano soggetti che manifestano un atteggiamento negativo verso il progetto. I risultati minimi da richiedere al Gruppo Analisi (sui quali potrà essere valutato) sono i seguenti:

- a. inventario dei procedimenti gestiti da tutti gli uffici comunali;
- b. indicazioni occorrenti per:
 - individuazione delle pratiche "sportellabili",
 - definizione della struttura dello Sportello,
 - individuazione delle risorse necessarie,
 - standardizzazione dei flussi procedurali e modulistica,
 - elaborazione dei "contenuti" (sportello fisico – sportello online).

- c. accrescimento professionale e culturale, creazione di una conoscenza diffusa sui vari servizi.

La scelta di gestire il progetto con risorse interne, ricorrendo a supporti esterni solo quando indispensabile, risulta strategica a livello organizzativo. Una criticità da non sottovalutare è la resistenza al cambiamento che va affrontata stimolando il coinvolgimento e la condivisione attraverso:

- percorso di counseling filosofico sui temi della comunicazione e del "benessere organizzativo";
- istituzione di un gruppo interno di miglioramento costituito da "volontari" che hanno il compito di tenere viva l'attenzione su questi temi;
- incontri periodici con l'Amministrazione e la Direzione;
- costante aggiornamento sull'evoluzione del progetto (newsletter apposita, presenza negli uffici del Gruppo Analisi e del responsabile, ecc.);
- attivazione di un "progetto intersettoriale", anche ai fini dell'erogazione della produttività individuale: ogni servizio vi partecipa in base alle sue competenze, quanto meno per le "interviste".

Il Gruppo Analisi, coordinato dal responsabile di progetto, deve essere in costante contatto con dirigenti e Amministrazione, coinvolti e partecipi in ogni fase realizzativa.

3. Analisi dei rischi e definizione dei livelli di accettabilità (tecnologia/normativa)

Un progetto innovativo come quello legato alla dematerializzazione dei procedimenti amministrativi con cittadini e imprese necessita di un'attenta valutazione da un lato dei costi-benefici introdotti dalla tecnologia e dall'altro dei "rischi" legali e normativi che l'utilizzo di tali strumenti può comportare.

Accettare ad esempio una richiesta relativa ad una concessione edilizia per un'abitazione, presentata via posta elettronica con allegato un modello pdf senza firma digitale (strumenti molto semplici e alla portata di tutti), potrebbe causare problemi legali all'amministrazione. Per evitare ogni possibile contenzioso si potrebbe ipotizzare l'utilizzo obbligatorio di firma digitale e Posta Elettronica Certificata per ogni domanda online visto, che in base alla normativa italiana, sono paragonabili, nel mondo cartaceo, alla firma autografa davanti a pubblico ufficiale e alla raccomandata con ricevuta di ritorno. Ma con questi strumenti i servizi online sarebbero utilizzati in modo intensivo o solo a scopo dimostrativo?

Per evitare di creare servizi online poco utilizzabili la scelta delle tecnologie da utilizzare non può prescindere da un'attenta analisi di ogni singolo procedimento per il quale vanno rilevati tutti gli aspetti che consentano di rendere l'uso delle tecnologie semplice, funzionale ed efficiente, relativamente al bacino di utenza interessato, garantendo allo stesso tempo un livello di rischio accettabile per l'amministrazione.

Una metodica utilizzabile per tale rilevamento è quella di definire una mappatura dei procedimenti che indichi:

- bacino d'utenza interessato;
- frequenza di utilizzo (numero di procedimenti annui);
- strumenti tecnologici maggiormente disponibili per il bacino di utenza;
- modalità di presentazione cartacea (semplificazione Basanini);
- indice di rischio (in una scala da 1 a 10).

Per ogni procedimento va quindi calcolato l'indice di rischio che misurerà, sulla base di una scala quantitativa, il livello di "rischio" accettato dall'amministrazione. Di norma vengono definiti tre livelli di rischio (indicanti le tecnologie consentite

per il livello), le cui soglie sono valutate in modo soggettivo dall'amministrazione (tolleranza al rischio) che prevedono:

- livello di rischio basso (Verde): indice di rischio da 1 a 5;
- livello di rischio medio (Giallo): indice di rischio da 6 a 8;
- livello di rischio elevato (Rosso): indice di rischio da 9 a 10.

Nel caso l'analisi descritta porti come risultato a pochi procedimenti "verdi" e tanti "rossi" sarà necessaria una revisione consapevole della "tolleranza al rischio" da parte dell'amministrazione al fine di non progettare un sistema perfetto dal punto di vista tecnologico e normativo ma poco fruibile da cittadini ed imprese.

4. Analisi del processo di workflow e del livello di complessità

Un rischio che si corre nell'adozione di sistemi informatici per la gestione dei procedimenti amministrativi è quello di decidere di adottare una soluzione applicativa che "conosca" in modo completo e rigoroso il flusso di lavoro per ogni possibile casistica. Questo approccio, che si definisce procedurale (workflow procedurale), richiede un'analisi particolarmente approfondita, e una fase di implementazione onerosa, da ripetere per ciascun tipo di procedimento. Con il rischio di dover "ritarare" continuamente il sistema per venire incontro a modifiche organizzative, normative, o per gestire eccezioni non previste.

Nella realtà molti procedimenti, in generale, sono spesso caratterizzati da una forte componente destrutturata, in cui cioè è richiesto di affrontare percorsi inusuali nella gestione della pratica, oppure coinvolgere servizi non previsti, o applicare nuove norme o regole molto specifiche.

Questo approccio, che delega completamente al personale dell'ente la definizione del flusso di lavoro, è chiamato collaborativo (workflow collaborativo), e garantisce elevata flessibilità

e semplicità nella fase di implementazione. Spesso rappresenta l'unica soluzione percorribile, a discapito però dei molti vantaggi legati al modello di Business Process Management (BPM).

La soluzione ottimale per la gestione dei procedimenti amministrativi prevede un nuovo modello “misto” (procedurale-collaborativo) in grado di mantenere inalterati i vantaggi del modello BPM evitando molte delle criticità evidenziate in precedenza. L'idea di base consiste nell'affrontare l'analisi di un processo con un approccio di tipo top-down identificando come primo passo le principali macro attività che lo compongono ed i relativi responsabili.

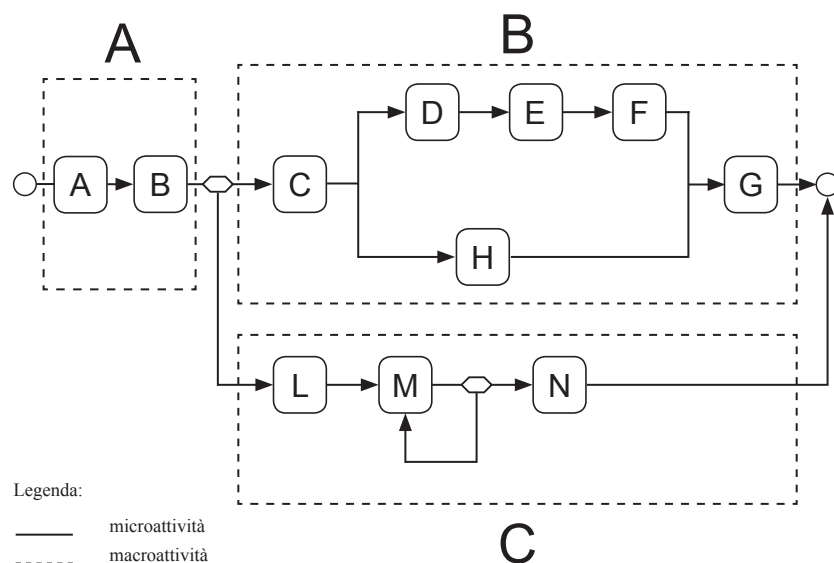


Figura 1. Modello procedurale-collaborativo

Il tutto porta ad un processo semplificato che consente di controllare il flusso delle macro attività garantendo per queste ultime il necessario livello di standardizzazione, tracciabilità, controllo delle tempistiche e misurazione delle performance.

L'approccio proposto prevede la gestione amministrativa di tutte le prestazioni offerte ai cittadini utilizzando un unico processo standard di alto livello, ricavato dall'analisi delle attività che sono comuni ad ogni procedimento, che controlla le fasi più importanti ma lascia la libertà di gestire gli aspetti specifici di ogni singolo procedimento mediante una procedura collaborativa.

Nella figura seguente viene schematicamente descritto il “macro-processo” dei servizi attivato dalla richiesta (online o cartacea) da parte di un cittadino, all'interno nella soluzione Siav denominata Koinè ed applicata concretamente nel progetto Incontr@Ciriè, che sarà trattato nella prossima relazione.

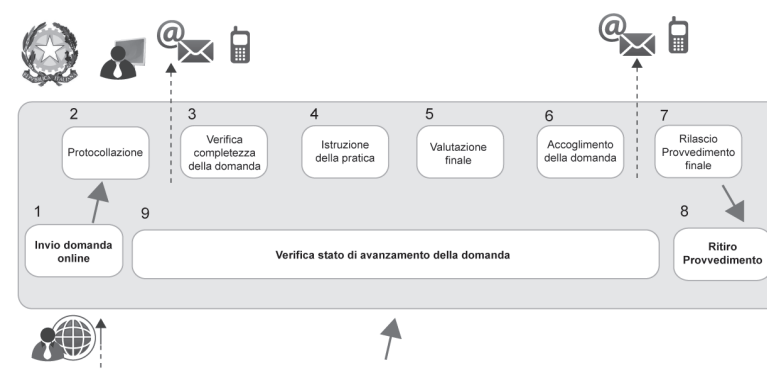


Figura 2. Il “macro-processo” dei servizi attivato dalla richiesta da parte del cittadino

Il “macro-processo” comune per tutti i servizi è caratterizzato dalle seguenti “macro-attività”:

1. **Protocolloazione:** si procede alla protocollazione della domanda che successivamente viene assegnata automaticamente all'ufficio di competenza per la successiva elaborazione. L'amministrazione comunica al cittadino, mediante SMS, le credenziali di accesso allo Sportello “virtuale” per consentirgli di verificare in autonomia lo stato di avanzamento della domanda.

2. Verifica completezza della domanda: l'ufficio competente provvede alla verifica della documentazione ricevuta e alla eventuale richiesta di documentazione integrativa.
3. Istruzione della pratica: la domanda del cittadino viene istruita dall'ufficio competente mediante l'utilizzo di "workflow collaborativo".
4. Valutazione finale: l'amministrazione verifica, in base ai risultati dell'istruttoria, se accogliere o respingere la domanda.
5. Accoglimento o Diniego della domanda: in caso di idoneità della domanda l'amministrazione procede all'accoglimento della stessa e completa la lavorazione della pratica altrimenti avvia un'interlocutoria di diniego.
6. Rilascio del Provvedimento finale o del Provvedimento di Diniego: l'amministrazione procede all'emissione del provvedimento finale di accoglimento o diniego.

All'interno di ogni "macro-attività" il sistema gestisce i percorsi specifici di ogni singolo provvedimento tramite l'utilizzo di "workflow collaborativi" che consentono agli utenti, anche esterni all'ufficio che sta lavorando la pratica o addirittura all'amministrazione, di effettuare le relative attività sui diversi procedimenti amministrativi.

La soluzione "ibrida" con workflow procedurale misto ad attività collaborative tra i servizi del back office consente di pubblicare online rapidamente e con semplicità tutti i procedimenti dell'amministrazione, con costi per singolo procedimento estremamente contenuti. Questo senza inficiare gli obiettivi di trasparenza e tracciabilità per il cittadino. Sia il "macro-processo" dei servizi sia i singoli "workflow collaborativi" sono trasversali alla struttura amministrativa: essi possono attraversare più amministrazioni e più servizi/uffici nella stessa amministrazione.

5. Misurazione delle performance (indicatori e sistemi di calcolo)

Il contesto in cui operano le amministrazioni pubbliche sta evolvendo rapidamente da una situazione di sostanziale stabilità ad una situazione dinamica che richiede di dover rispondere adeguatamente e in maniera tempestiva alle crescenti esigenze da parte delle imprese, dei cittadini ed in generale di tutti gli interessati.

Le amministrazioni sentono sempre più l'esigenza di poter valutare le performance di tutta la macchina amministrativa dove la "misurazione" viene vista in chiave migliorativa, come fonte di informazioni significative sia per la gestione interna sia per il servizio reso all'utenza.

In un modello reale di amministrazione dematerializzata le richieste da parte di cittadini ed imprese saranno digitali e cartacee: probabilmente quelle cartacee continueranno ancora per qualche anno ad essere predominanti anche se con il cambio generazionale questa proporzione tenderà ad invertirsi (generazione internet).

Appare quindi evidente che un sistema informatico che vuole proporsi come strumento di governance della macchina amministrativa non può trascurare le istanze presentate in modo cartaceo e quindi il modello deve prevedere un unico punto di ingresso (cartaceo/digitale), che di norma è rappresentato dal protocollo, dal quale poi vengano attivati i processi gestionali che siano identici sia per le richieste cartacee presentate allo sportello fisico, che per quelle digitali pervenute attraverso lo sportello virtuale.

Se ad esempio il processo di gestione per l'iscrizione all'asilo nido prevede che alla protocollazione della domanda venga avviato un processo di workflow che notifica l'avvenuta pro-

tocollazione con un SMS e pubblica sul portale (area riservata) sia il documento di richiesta che la comunicazione di avvio procedimento, queste attività dovranno essere svolte anche per la domanda cartacea.

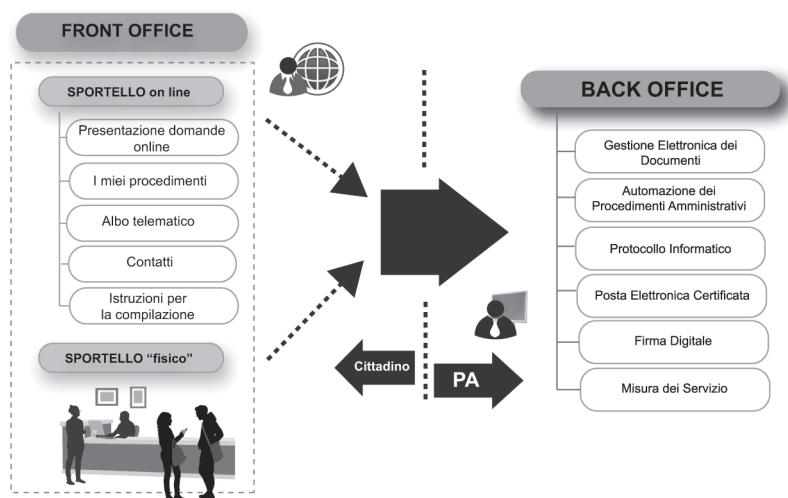


Figura 3. Modello di sistema informatico front office/back office

Progettando l'infrastruttura in questo modo è possibile quindi standardizzare il processo di lavorazione di tutte le domande presentate, qualunque sia il canale scelto, raccogliendo in modo automatico e strutturato tutte le informazioni necessarie che potranno successivamente essere utilizzate a fini statistici per la quantificazione degli indici di performance (KPI) definiti dall'amministrazione nel suo piano di qualità.

Si ringrazia lo studio di consulenza Archimed di Bressanone (BZ) per il prezioso contributo offerto nello sviluppo delle idee presentate.

Marina Macario

Dematerializzare il rapporto con i cittadini: una scelta organizzativa prima che tecnologica. Un'esperienza reale

Marina Macario

Dopo aver iniziato la sua attività come analista programmatrice, Marina Macario è stata per molti anni responsabile CED del Comune di Ciriè, fino a divenire responsabile di servizio a seguito della riorganizzazione interna avvenuta nel 2007. Ha coordinato, come consulente esterna, i progetti di informatizzazione di alcuni consorzi. Si è inoltre dedicata ad attività in ambito statistico e di controllo di gestione. Da sempre promotrice dell'innovazione nella PA, ha partecipato attivamente a numerosi progetti specifici in materia di nuove tecnologie, comunicazione e qualità. Ha gestito, insieme al dirigente Gianni Bergantin, le fasi progettuali e realizzative del progetto Incontr@ciriè, in tutti i suoi aspetti tecnologici, logistici ed organizzativi. In questo ambito ha coordinato per tre anni il Gruppo di lavoro interno, le attività di rilevazione e analisi, la predisposizione dei nuovi ambienti e la transizione verso i nuovi sistemi. Attualmente è Responsabile del Servizio Sistemi informativi e Comunicazione del Comune di Ciriè (Torino).

Il primo marzo 2011 rappresenta per la Città di Ciriè una data da ricordare. È stato infatti il primo giorno di effettiva operatività del nuovo Sportello Incontr@ciriè, risultato di un ambizioso progetto che ci ha impegnati negli ultimi anni.

Qualche indicazione sulla nostra realtà può essere utile a contestualizzare questo intervento: Ciriè è un Comune di circa 19.000 abitanti situato a 21 Km da Torino e a 7 Km dall'aeroporto Perini. Importante centro commerciale e di servizi, sede di ASL, scuole superiori di ogni genere, uffici giudiziari, Agenzia Entrate, CCIAA e di numerosi altri enti pubblici, si connota come realtà di riferimento per le Valli di Lanzo e il basso Canavese.

Incontr@ciriè è un servizio innovativo, che cambia radicalmente il modo di rapportarsi con il Comune. Uno sportello davvero

“unico” e polifunzionale, che gestisce il front office di tutti gli uffici comunali grazie a un patrimonio di “conoscenza condivisa” digitale, creato e gestito utilizzando la “dematerializzazione” come fulcro del progetto per migliorare e potenziare i servizi resi agli utenti.

La denominazione “Incontr@cirié” richiama lo spirito che ha animato la nascita di questo nuovo sportello, che vuole essere uno sportello per i cittadini, i professionisti, le aziende: un segno politico della centralità di questi soggetti, che si sviluppa in sintonia con le evoluzioni e i cambiamenti in corso nella pubblica amministrazione, rivolti alla semplificazione e alla trasparenza, a rendere “più vicino” il Comune alla gente: un progetto scaturito dalla volontà di agevolare il rapporto con i cittadini, e di migliorare la qualità dei servizi erogati, razionalizzando e ottimizzando nel contempo l’operatività interna e riducendo i costi complessivi.

Incontr@cirié è costituito da due sportelli fisici, Sportello del Cittadino e Sportello delle Imprese – SUAP TerritorioImpresa, che si distinguono soltanto per la tipologia di utenza (cittadini e professionisti per il primo, aziende per il secondo). Sono stati infatti progettati e strutturati in modo univoco, con le stesse attività preliminari e il supporto degli stessi strumenti tecnologici. Ai due sportelli fisici si affianca Incontr@cirié on line, che offre su Web gli stessi servizi, 24 ore su 24.

Una struttura come Incontr@cirié, oltre a fondarsi su precise scelte organizzative e progettuali, deve possedere alcuni requisiti essenziali: essere multicanale, basarsi su soluzioni tecnologiche all’avanguardia, avvalersi di una solida piattaforma di gestione documentale e di workflow, prevedere una revisione attenta e costante dei procedimenti e della modulistica, crescere nel tempo con continuità, senza mai fermarsi.

La prima idea di creare uno “Sportello Unico”, visto inizialmente come evoluzione dell’URP, si sviluppò nel nostro comune

all’inizio del 2007, innestandosi sul progetto di digitalizzazione della gestione documentale al quale stava lavorando il servizio sistemi informativi. In sintesi, ci si rese conto che il sistema già individuato per razionalizzare la gestione documentale e amministrativa ben si prestava a supportare il nuovo servizio di front office, migliorando l’interazione con gli interlocutori esterni. La “dematerializzazione”, accompagnata da un cambiamento culturale e da un ammodernamento delle modalità di rapporto con l’utenza, può così dispiegare appieno le sue potenzialità, fornendo risultati importanti e tangibili sia all’interno della struttura comunale, sia in termini di servizio e di immagine della PA. La digitalizzazione dei documenti, spesso finalizzata esclusivamente alla diminuzione degli scambi cartacei e della consistenza degli archivi, diventa così strumento di performance e qualità per l’ente.

Lo “Sportello Unico” si connota come sportello “esperto”, in grado di abbinare all’informazione una vera e propria “consulenza” al cittadino. Parliamo insomma di una struttura demandata a costituire il riferimento privilegiato per le principali transazioni tra cittadini e Comune. Un nuovo servizio che, grazie al patrimonio informativo di cui dispone tramite la piattaforma di gestione documentale e di workflow, è in grado di risolvere in un unico luogo problemi anche complessi. Lo sportello deve essere “esauriente”, ossia garantire all’utenza tutte le prestazioni che, in concreto, non presentano impedimenti davvero insuperabili per l’erogazione in tale sede.

In realtà, lo Sportello Unico è stato il risultato più evidente di un complesso processo di revisione e razionalizzazione che, ponendo mano ai meccanismi organizzativi e gestionali interni, ha eliminato alcune palesi criticità, che si ponevano in aperto contrasto con le crescenti esigenze degli utenti, ai quali gli sportelli tradizionali apparivano ormai inadeguati.

Il progetto, insomma, è stato concepito e configurato per trovare risposta a una pluralità di problematiche, tra loro strettamente interdipendenti. In particolare:

- necessità di migliorare i servizi erogati, con orientamento all'efficienza, all'efficacia e alla trasparenza;
- esigenza di semplificare i rapporti tra cittadini e PA, anche mettendo concretamente a disposizione strumenti che consentano l'utilizzo di nuovi canali per interagire con il Comune, in modo vantaggioso sia per gli utenti che per gli operatori comunali;
- esigenza di razionalizzare l'organizzazione interna, con introduzione di flussi procedimentali e documentali strutturati;
- necessità di ottimizzare l'utilizzo delle risorse umane senza penalizzare la qualità, anzi migliorandola (affrontata attraverso lo sviluppo delle professionalità, la diffusione di una nuova "cultura", la preparazione di operatori più "polifunzionali" e "intercambiabili", la disponibilità di una piattaforma digitale di "conoscenza condivisa" completa, semplice e costantemente aggiornata, accessibile anche ai cittadini attraverso il portale Incontr@cirié);
- esigenza di razionalizzazione della gestione dei documenti: stop alle lunghe ricerche su documenti cartacei, stop ai documenti "sparsi", alle mille copie di modelli non più aggiornati, alle pratiche cartacee chiuse nei cassetti;
- necessità di ottimizzare la gestione archivistica, con l'introduzione di meccanismi di classificazione e fascicolazione automatica dei documenti digitalizzati e dei "procedimenti".

Il primo consistente intervento di riorganizzazione interna fu attuato all'inizio del 2007. Questo intervento, tra l'altro, fece confluire nel nuovo Servizio Sistemi Informativi e Comunicazione (collocato nel settore Economia e Organizzazione) gli uffici

URP, protocollo, archivio, sistemi informativi e comunicazione. In questo modo tutti questi uffici, assolutamente strategici per il progetto Sportello, vennero accentrati in un'unica struttura e con un unico responsabile, scelta che indubbiamente facilitò la fase decisionale della progettazione complessiva.

Sin dal primo avvio del progetto, si capì che riorganizzazione interna e adozione di piattaforma GED non sarebbero state sufficienti a garantirne il buon esito. In particolare, fu subito chiaro il ruolo strategico rivestito dalla comunicazione, e in particolare dalla comunicazione interna, per creare il clima adatto all'introduzione di meccanismi di semplificazione e alla diffusione della "cultura del cambiamento". A questo proposito, il comune di Cirié aveva già attuato nel 2005 un percorso formativo di "counseling filosofico", esteso a tutti i dipendenti e agli amministratori e mirato a sviluppare il concetto di "benessere organizzativo", che si concluse con l'adozione di una "carta etica" e la creazione di un "Gruppo interno di miglioramento" per tenere desta, in tutti i servizi comunali, l'attenzione e la sensibilità verso queste importanti tematiche. I risultati di questo percorso si sono rivelati preziosi ed essenziali per avviare e realizzare le innovazioni programmate.

Non bisogna infatti dimenticare che il primo ostacolo da superare per portare a compimento progetti che comportano sconvolgimenti e grandi novità, è rappresentato dalla resistenza interna al cambiamento. Bisogna individuare mezzi e modalità per superare la cultura "della forma" in favore di una cultura dell'innovazione, dell'evoluzione e della crescita continua. Da questo punto di vista, la scelta di agire sulla comunicazione, sulla formazione e sul coinvolgimento attivo di tutti si è rivelata vincente.

Il coinvolgimento attivo, nel Comune di Cirié, divenne realtà attraverso la scelta di realizzare internamente la maggior parte delle fasi progettuali, ricorrendo a supporti esterni solo quando indispensabile.

Questa scelta fu dettata principalmente da due considerazioni:

- un progetto complesso come quello in questione, per andare a buon fine, non può prescindere dall'interesse e dalla condivisione di tutta la struttura dell'ente;
- la gestione interna del progetto, realizzata avvalendosi dei dipendenti comunali, rappresenta un indubbio valore aggiunto in termini di crescita professionale, di sviluppo di conoscenze e di apertura al "nuovo" e alle più moderne tecnologie: un patrimonio che non va disperso, vantaggioso anche a lungo termine.

Fu quindi per queste ragioni che si decise che il progetto fosse portato avanti da un "gruppo di lavoro" intersettoriale, costituito inizialmente da una decina dipendenti affiancati poi dagli "sportellisti", ossia dai colleghi selezionati (in base a criteri di volontarietà, esperienza e attitudine) per diventare operatori di Incontr@cirié.

Questo gruppo di lavoro, opportunamente formato, si è fatto carico di alcune attività basilari: rilevazione dei procedimenti, segnalazione delle criticità, raccolta e revisione della modulistica, supporto all'adozione della nuova piattaforma di gestione informatizzata di documentazione e workflow nei vari servizi comunali. Si è inoltre fatto promotore del progetto all'interno della struttura comunale, favorendo la comunicazione interna relativa a finalità e sviluppi e mantenendo alta l'attenzione dei colleghi.

Credo sia a questo punto indispensabile sottolineare che il progetto "Sportello Polifunzionale", sostenuto dalla forte volontà del Sindaco e della Giunta e condiviso dai dirigenti, è stato veramente un progetto di tutta la struttura. Infatti, sebbene le attività principali siano state demandate al gruppo di lavoro tutti i colleghi sono stati chiamati a contribuire con il loro apporto: nelle interviste durante la fase di rilevazione dei procedimenti,

nella revisione della modulistica, nell'adeguamento dell'organizzazione e delle modalità operative alle implicazioni connesse ai nuovi sistemi di gestione dei documenti e dei procedimenti, nel farsi carico di alcune attività "ordinarie" in sostituzione di chi era impegnato nel gruppo di lavoro.

Proprio per questo, il progetto "Sportello Polifunzionale" è stato per alcuni anni un "obiettivo intersettoriale" per l'assegnazione del compenso incentivante la produttività.

La partecipazione collettiva è stata sempre sostenuta attraverso numerose azioni mirate di comunicazione interna, newsletter specifica e incontri periodici (anche con l'Amministrazione) in primis.

Ma torniamo alle origini, per approfondire cosa sta dietro allo "Sportello Incontr@cirié" e raccontarne in sintesi la storia.

La realizzazione di uno "Sportello Polifunzionale" con le connotazioni di Incontr@cirié implica necessariamente una serie di attività importanti e impegnative, quali:

- rilevazione, analisi e reingegnerizzazione dei procedimenti;
- selezione e attivazione di un sistema informatizzato di gestione documentale (produzione del documento, protocollazione, smistamento, archiviazione, ricerca) esteso a tutti i servizi comunali;
- raccolta sistematica e digitalizzazione dei contenuti di "informazione" e "conoscenza" con creazione di una piattaforma di "conoscenza condivisa", disponibile a tutti attraverso il sistema GED;
- adeguamento delle infrastrutture informatiche e telematiche;
- informatizzazione della gestione procedimentale, con definizione delle fasi demandate al front e al back office;
- progettazione dello "Sportello": logistica, arredi e attrezzature, orari, organizzazione, ecc.

- progettazione e predisposizione dello Sportello on line;
- selezione e formazione del personale addetto allo “Sportello”;
- realizzazione pratica della nuova struttura.

Nella nostra realtà, anche in conseguenza della scelta di sviluppo interno e di obiettive limitazioni economiche (i costi sono rilevanti, e nel nostro caso sono stati interamente coperti con risorse comunali, dall’acquisto degli strumenti a quello dei nuovi locali destinati a ospitare lo sportello fisico), il progetto si è sviluppato su un triennio, iniziando a gennaio 2008 con l’introduzione del nuovo protocollo informatico e l’avvio della digitalizzazione dei documenti in ingresso.

In questa occasione è stato adottato un nuovo titolario di classificazione, basato sui servizi e sulle prestazioni erogati dal Comune: un importante tassello per raggiungere i risultati attesi, con un occhio di riguardo alla gestione archivistica.

Nello stesso anno, dopo un breve periodo di formazione/affiancamento da parte di una società specializzata in ingegneria gestionale, sono state definite le tecniche e le modalità operative per gli interventi di rilevazione e analisi dei procedimenti.

Ritengo opportuno evidenziare che sia la progettazione del materiale di rilevazione (schede, flow chart, ecc.) sia l’individuazione degli elementi da rilevare (attività, riferimenti normativi, criticità segnalate o emerse, modulistica, frequenza e particolarità, presenza di figure specialistiche, ecc.) sono state tarate sull’obiettivo “Sportello”: quindi la reingegnerizzazione dei procedimenti è stata vista non come fine a se stessa, ma come parte di un progetto che deve portare le fasi di input-output e informazione di ogni procedimento a uno “Sportello Unico”.

Il 2008 e il 2009 sono stati dunque dedicati a rilevazione e analisi dei procedimenti (oltre 250 trattati, oltre 200 individuati come gestibili allo sportello), selezione e formazione del personale,

individuazione dei locali e progettazione del loro allestimento, sviluppo della piattaforma di gestione documentale informatizzata e del suo utilizzo diffuso nei vari servizi, “sincronizzazione” degli archivi cartacei e digitali, validazione e reingegnerizzazione delle procedure, uniformazione della modulistica, definizione del layout e dei contenuti dello Sportello on line.

Nel frattempo, la gestione digitale è stata estesa ai documenti in uscita e a quelli prodotti internamente: in pratica, tutti i nuovi documenti prodotti o ricevuti sono ora disponibili in versione digitale, dove e quando servono, ai soggetti che sono autorizzati a “vederli”.

Il 2010 è stato dedicato agli interventi infrastrutturali, al potenziamento del sistema informatico e telematico, all’acquisizione dei nuovi locali e al loro allestimento, alla progettazione e all’acquisto degli arredi, alla definizione, alla verifica e al caricamento dei contenuti dello “Sportello Telematico”, all’affinamento della modulistica standard utilizzata anche dal back office per l’automazione dei flussi procedurali, all’individuazione di un “logo” caratterizzante e di un’immagine coordinata, alle azioni di comunicazione e informazione nei confronti di cittadini, professionisti, imprese e altri soggetti operanti sul territorio.

I futuri operatori degli sportelli hanno nel frattempo completato la loro formazione, anche attraverso la partecipazione diretta alle attività sulla modulistica e mediante periodi di “affiancamento” presso gli uffici comunali. Una scelta adottata anche per far sì che gli operatori si sentissero “parte attiva” nelle scelte e nella preparazione del servizio al quale avrebbero dovuto lavorare, evitando la percezione di un qualcosa di “calato dall’alto”.

Abbiamo inoltre realizzato un collegamento in fibra ottica tra le varie sedi comunali, attestato presso il nuovo CED completamente rivisto. Sulla nuova rete in fibra transitano ora in sicurezza i flussi di dati, le conversazioni vocali, il traffico Internet

e quello relativo ai sistemi di videosorveglianza. Insieme alla piattaforma di gestione documentale, essa garantirà continuità di servizio e prestazioni eccellenti agli Sportelli fisici e allo Sportello on line.

Ma cos'è, ora, lo Sportello Incontr@cirié?

Dal primo marzo 2011, tutti i procedimenti di front office relativi a cittadini e professionisti sono passati allo Sportello Incontr@cirié.

Nella stessa data è entrato in funzione Incontr@cirié on line, il nuovo portale semplice e chiaro, progettato con particolare attenzione all'accessibilità. Fornisce informazioni esaurienti sui procedimenti, sulla normativa e sulla modulistica. Permette di avviare da casa, 24 ore su 24, oltre 150 pratiche, nella maggior parte dei casi senza necessità di integrazioni allo sportello fisico. Ogni cittadino può verificare on line lo "stato di avanzamento" delle sue pratiche con l'opportunità di visualizzare in un vero e proprio "fascicolo elettronico" i documenti relativi, contattare il comune via email, ricevere SMS di avviso per l'avvio del procedimento piuttosto che per la sua conclusione: questi nuovi strumenti di comunicazione stanno diventando, giorno per giorno, i canali privilegiati di interazione con cittadini, aziende e professionisti.

La "dematerializzazione", normalmente introdotta per ridurre i consumi di carta o i volumi degli archivi, ora è davvero al servizio dei cittadini e della struttura comunale.

E la "dematerializzazione" inizia proprio allo Sportello Incontr@cirié, che prende in esame le istanze pervenute attraverso il portale, ne controlla compilazione e allegati, protocolla e avvia il flusso procedimentale. Identica procedura viene applicata alle istanze consegnate allo sportello o arrivate via posta tradizionale, PEC o fax. Le attività di front office non si limitano però alla verifica e

all'accettazione dei documenti: gli sportellisti gestiscono di fatto le fasi di input-output per la quasi totalità dei procedimenti comunali, indipendentemente dal settore di riferimento. Se mancano allegati obbligatori contattano il richiedente, in modo da passare al back office una documentazione completa. Tutti i documenti vengono "allegati" al procedimento. Poiché i procedimenti sono nativamente classificati all'interno di una specifica voce di titolo, i relativi documenti vengono automaticamente classificati, e fascicolati. Gli operatori di back office prendono in carico i procedimenti e ne gestiscono le varie fasi utilizzando gli automatismi forniti dalla piattaforma di workflow e i modelli standard.

Tutta la "filiera" della gestione documentale diventa dunque digitale: lo sportello fisico digitalizza tutti i documenti che arrivano in formato cartaceo (allo sportello, via posta, ecc.) e avvia il procedimento per le istanze pervenute. Le pratiche vengono gestite, con documenti digitali, dal back office, per poi tornare allo Sportello per la consegna del provvedimento finale e la chiusura del procedimento. Gli sportellisti sono in grado di operare sulle pratiche di tutti i settori comunali, grazie a una piattaforma di "conoscenza condivisa" completamente digitale, che costituisce il punto forte di tutto il progetto.

Molti, e importanti, sono quindi i risultati e i risparmi conseguiti con Incontr@cirié.

- Miglioramento del servizio reso agli utenti, che ora trovano sul portale Incontr@cirié tutto quanto occorre per avviare e seguire on line oltre 150 tipologie di procedimento.
- Maggiore trasparenza: il patrimonio informativo, raccolto e costruito durante il progetto, è a disposizione di tutti: degli sportellisti, dei dipendenti comunali, dei cittadini e delle aziende.
- Enfasi sull'utilizzo degli strumenti informatici nell'interazio-

ne con la PA: tutto il progetto è stato orientato in questa direzione, mirato a far percepire la PA come realtà moderna, funzionale, snella e soprattutto “aperta” verso i suoi interlocutori.

- Miglioramento organizzativo interno: utilizzando il sistema di gestione documentale e di workflow si standardizzano le modalità operative e la modulistica, la conoscenza diventa diffusa e i responsabili acquisiscono nuovi agevoli strumenti di azione sulla gestione dei procedimenti e sui relativi tempi.
- Standardizzazione: della modulistica, dei procedimenti, delle principali modalità di lavoro, collaborazione e scambio tra i vari uffici comunali, oltre che del rapporto con l'utenza.
- Analisi e misurazione performance e soddisfazione utenti: il sistema di gestione documentale e di workflow adottato dal Comune di Cirié comprende strumenti integrati di analisi, monitoraggio, statistica e misurazione di performance costi e qualità, che saranno progressivamente attivati a partire dai prossimi mesi, nell'ottica del miglioramento continuo.
- Costi del personale: gli operatori sono polifunzionali, effettivamente intercambiabili e quindi tendenzialmente meno numerosi. È diminuito l'impegno di risorse umane in ricerche di archivio, smistamento di documenti cartacei ecc. Si attendono poi risultati concreti (diminuzione dell'afflusso agli sportelli fisici in primis) dalla promozione e diffusione dell'utilizzo di strumenti informatici e telematici, e dalla standardizzazione/automazione del workflow.
- Costi di gestione archivistica: non vengono prodotte più copie di uno stesso documento, i fascicoli sono organizzati in modo strutturato per facilitare l'archiviazione e il reperimento dei documenti. In prospettiva si genererà sempre meno carta, per cui si otterranno risparmi anche sui volumi degli archivi e sulla conseguente occupazione di spazi.

- Costi di stampa (dispositivi, toner, carta): sempre più documenti digitali “nativi”, sempre meno documenti cartacei in tutti i contesti.
- Costi di affrancatura e postalizzazione: i canali privilegiati per l'interazione sono ora la posta elettronica, la PEC e gli SMS.

L'apertura dei nuovi sportelli Incontr@cirié, risultato senz'altro ambizioso, sarà seguita da ulteriori attività di completamento e miglioramento del progetto: attività concentrate sulla gestione dei flussi procedurali, sull'ottimizzazione dell'utilizzo della piattaforma di gestione documentale e della posta certificata, sull'implementazione di strumenti per la rilevazione della customer satisfaction e per il controllo di gestione. Nei prossimi mesi crescerà considerevolmente anche il numero di procedimenti gestiti allo Sportello (e presenti sullo Sportello on line), con l'aggiunta di alcune decine di voci relative al SUAP (Sportello Unico Attività Produttive, che lavora per Cirié e altri dieci comuni). Queste attività ci coinvolgeranno sia negli ultimi mesi del 2011 che negli anni successivi: l'apertura dello Sportello è un primo importante traguardo, ma l'evoluzione deve continuare per non vanificare i risultati ottenuti.

Questi risultati stanno peraltro confermando la validità del progetto: il servizio funziona senza intoppi, gli utenti dimostrano il loro apprezzamento, il back-office ha assimilato i nuovi strumenti e li utilizza in modo appropriato. Passato il primo mese di “rodaggio”, il giudizio complessivo non può essere che positivo.

Questa la situazione attuale:

- sportello del Cittadino: 6 postazioni + reception;
- apertura al pubblico: oltre 25 ore settimanali, sabato incluso;
- oltre 150 i procedimenti gestiti allo Sportello (informazione, modulistica, input-output);
- portale Incontr@cirié: uno sportello accessibile, aperto 24 h su 24;

- pratiche relative a tutti i settori comunali (demografici, tecnici, politiche sociali, istruzione, ambiente ecc.);
- lo Sportello Incontr@cirié assolve tutte le funzioni di front office: gli altri uffici comunali sono chiusi al pubblico;
- postazioni e operatori realmente “polifunzionali”, intercambiabili;

Infine, qualche numero, riferito a fine giugno 2011 e quindi a quattro mesi dall'apertura dello sportello, per dare la misura dell'andamento di Incontr@cirié:

- circa 8000 gli accessi allo Sportello del Cittadino;
- tempi di attesa sempre inferiori ai 10 minuti;
- circa 2500 i procedimenti avviati e gestiti con i nuovi sistemi;
- oltre 300 i procedimenti avviati attraverso il portale.

Michele Petrocelli

L'informatizzazione dei processi di gestione del personale come strumento per la valorizzazione del servizio offerto: il caso MEF

Michele Petrocelli

Laureato in Economia, Dottore di Ricerca in Economia e Finanza nel governo dell'impresa è attualmente dirigente presso il Ministero dell'Economia e delle Finanze-Dipartimento dell'Amministrazione Generale, del Personale e dei Servizi e titolare delle cattedre di Economia Politica e di Economia Monetaria presso l'Università Guglielmo Marconi, dove assume il ruolo di Direttore Scientifico di diversi Master. Ha partecipato, in ambito OCSE, a progetti internazionali di ricerca su sistemi di budgeting, governance pubblica e di gestione delle risorse umane.

Mi è stato chiesto di raccontare l'esperienza maturata nel progetto di riorganizzazione dell'Ufficio che attualmente dirigo. Nel farlo spero di condividere non solo, e non tanto, il processo di innovazione dei processi, quanto le conseguenze organizzative che esso porta con sé.

Nell'ambito del Ministero dell'Economia e delle Finanze, l'Ufficio VII della Direzione Centrale per i Servizi al Personale, composto di 90 persone che dirigo da due anni e mezzo, rappresenta per circa 13.000 dipendenti attualmente in servizio, nonché per i cessati provenienti dalle altre Amministrazioni nel tempo confluite nei ruoli del Ministero dell'Economia e delle Finanze, un punto di riferimento importante per la gestione degli aspetti connessi con il trattamento giuridico del personale, quali la ricostruzione di carriera e del profilo professionale, il riconoscimento delle mansioni superiori, la ricostruzione dello stato matricolare e curriculare, la tenuta dei fascicoli cartacei ed informatici, il rilascio di attestazioni di servizio, tessere di riconoscimento, autorizzazioni a svolgere incarichi, calcoli di anzianità.

Questo Ufficio è stato oggetto di un processo di completa ristrutturazione che ha cercato di trovare nella dematerializzazione una chiave di volta importante, per recuperare efficienza e qualità in un contesto di continuo ampliamento del suo servizio, con parallela riduzione delle risorse disponibili.

Si pensi, a titolo di esempio, che nel solo anno 2010 sono pervenute richieste per attestazioni di servizio pari a 4 volte quelle registrate nell'anno precedente, sono state lavorate il triplo delle posizioni matricolari e curriculari e rilasciato il doppio dei calcoli di anzianità.

La volontà di fornire un servizio in linea con le aspettative dell'utenza, sia dal punto di vista quantitativo che qualitativo, la necessità di ridurre i costi e i tempi delle tradizionali procedure ed il bisogno di superare le rigidità organizzative interne rappresentano le ragioni poste a fondamento di un importante e complesso processo di cambiamento.

Tale processo fa della dematerializzazione dei flussi di lavoro e della *lean organization* i suoi pilastri fondamentali, mediante i quali presidiare in modo evolutivo ed efficace le attività istituzionali, segnando standard qualitativi elevati.

La visione generale è stata costruita e condivisa con i dipendenti dell'Ufficio, la cui adesione ha rappresentato il vero valore aggiunto dell'intera iniziativa.

La prima lezione che ho tratto subito da questo progetto: è necessario che accanto all'innovazione tecnologica e organizzativa ne occorre sempre una culturale, altrimenti, se le persone subiscono l'innovazione, senza comprenderla, apprezzarla, farla propria, finiscono per distorcerla, rendendola inefficiente. Se le persone non capiscono il senso di una innovazione, questa non funzionerà, distruggerà anziché creare valore. Quando avevo davanti un passaggio importante del progetto, quindi, mi sono chiesto se le

persone l'avrebbero fatto proprio. A quel punto, se la risposta era no, avevo due strade: se il contributo potenziale dell'innovazione era minimo, preferivo abbandonarlo, se il contributo potenziale era elevato sarebbe stato necessario spendere tutte le energie possibili per farlo capire. Poiché le persone sono normalmente ragionevoli, di solito più sono i vantaggi meno ci vuole per far loro abbandonare una vecchia serena procedura consolidata.

Il cambiamento, poi, ha ruotato intorno ad un'altra idea portante che abbiamo sintetizzato nel motto "provare a diventare invisibili". Questo significa rendere tangibile ed accessibile il servizio, ossia consentire agli altri Uffici, ai dipendenti e a tutti i destinatari dei servizi resi di acquisire in tempi certi ed in modo agevole tutte le informazioni necessarie circa lo stato di avanzamento di ciascuna pratica, interagendo direttamente con il personale solo nel caso di particolari esigenze e rendendo, in tal modo, il contatto telefonico rarefatto, eventuale, legato a necessità stringenti, con vantaggi elevatissimi in termini di produttività sul lavoro.

A tale scopo, è stato adottato un sistema di tracciamento delle pratiche, basato su una banca dati interna ed alimentata dalle informazioni inserite e periodicamente aggiornate da tutti gli operatori. Il database, oltre a facilitare la gestione della singola pratica da parte del soggetto competente, consente, attraverso molteplici criteri di ricerca, la sua individuazione in ogni fase del processo di lavorazione, con contestuale possibilità di rilascio di tempestive informazioni, anche da parte di chi è estraneo alla lavorazione.

In sostanza, oltre ad una sensibile riduzione delle richieste, oggi possiamo stimare che, delle problematiche sollevate telefonicamente dall'utenza, il 70% viene evaso dalla mia segreteria (che, appunto, accede ai database e che oggi rappresenta un punto di contatto per l'intera giornata lavorativa con chiunque necessiti informazioni) e solo per il 30% è necessario mettere il dipendente in contatto con il responsabile delle pratiche, consentendo

al richiedente di avere risposte tempestive, efficaci, risolutive e ai responsabili dei procedimenti di poter lavorare tranquilli (e quindi di più e meglio).

Ma l'argomento forte di questa riorganizzazione risiede nel progetto di dematerializzazione dei processi gestiti. Si è focalizzata l'attenzione, in particolare, sulla definizione, pianificazione e predisposizione di nuove prassi che, tramite l'ausilio di sistemi operativi già esistenti e l'introduzione e l'utilizzo di nuovi strumenti, quali la firma digitale, la securizzazione e la Posta Elettronica Certificata, hanno reso possibile uno snellimento delle procedure con conseguente incremento dell'efficacia dell'azione amministrativa.

L'obiettivo, pertanto, è stato interpretato non solo in termini di semplice dematerializzazione della fase di acquisizione delle istanze, ma, più in generale, in un'ottica di integrale informatizzazione dei processi di interesse dell'Ufficio, compresi quelli non attivati ad istanza di parte.

Il riferimento è, in particolare, ad alcune attività tipiche, di cui darò qui brevemente conto, quali la ricostruzione dello stato matricolare e curricolare, il rilascio di attestazioni di servizio per uso personale o professionale, la gestione della raccolta dei decreti relativi a ciascun dipendente.

I diversi progetti che l'Ufficio, in collaborazione con CONSIP e con la Direzione Centrale dei Sistemi Informativi e dell'Innovazione, ha intrapreso già a partire dal 2010 ed implementato nel corso di quest'anno rispondono all'esigenza di semplificare tali processi mediante la loro digitalizzazione, integrando e, conseguentemente, valorizzando le informazioni.

Ogni lavorazione deve servire ad adempiere i fini istituzionali al massimo della qualità e tempestività possibile, cercando di mantenere per altre o future lavorazioni tutte le informazioni acquisite.

Il principio organizzativo che ci siamo dati, sfidante per molti di noi, è stato quello di "smettere di lavorare per la propria scrivania ed iniziare a lavorare per l'intera Amministrazione". Ogni persona deve capire esattamente cosa il proprio contributo significa non solo rispetto all'evasione della pratica assegnata, non solo rispetto alle istanze dell'utenza, ma anche nei confronti dell'organizzazione tutta, e del vantaggio che tale comportamento può dare al lavoro di tutti.

In primo luogo, uno strumento utilizzato è quello della securizzazione (dello stato matricolare e, prossimamente, degli attestati di servizio) con firma digitale ed apposizione dei relativi "glifi".

Il passaggio dal supporto cartaceo a quello digitale reca con sé due problematiche: da un lato, assicurare il corretto trattamento dei dati personali contenuti nello stato matricolare e, dall'altro, dar vita ad un documento che, una volta stampato, venga accettato anche all'esterno dell'Amministrazione che lo ha prodotto, consentendone la circolazione sia su supporto informatico che cartaceo.

La soluzione proposta per il rilascio dello stato matricolare, già pienamente operativa, consente di produrre in tempi rapidi un documento amministrativo in formato digitale idoneo a soddisfare tutti i requisiti di validità previsti dalla legge, grazie al sistema di contrassegno elettronico.

Oltre all'evidente risparmio in termini di tempo, la nuova procedura reca l'ulteriore vantaggio dell'abbattimento dei costi sostenuti per la spedizione cartacea, sostituita dalla trasmissione, mediante PEC, dello stato matricolare direttamente all'indirizzo di posta elettronica dell'interessato.

Analoghi benefici deriveranno dalla digitalizzazione del processo di rilascio delle attestazioni di servizio, prima, e di tutti i servizi all'utenza forniti dall'Ufficio, subito dopo.

Allo stato attuale, l'Ufficio, dopo la prima fase di analisi e revisione dei flussi documentali ed informativi, ha ultimato anche la seconda fase di definizione e pianificazione delle attività operative conseguenti alla completa informatizzazione del processo e si prepara, con il rilascio dell'applicativo da parte delle altre strutture interessate, alla definitiva realizzazione a sistema.

La messa in opera del progetto ci permetterà di semplificare il tradizionale iter di rilascio delle attestazioni di servizio, sostituendolo con una procedura interamente on-line che consentirà una riduzione dei tempi complessivamente necessari ad evadere le richieste, stimata in misura pari all'80%.

Al riguardo, occorre rilevare che il procedimento di rilascio delle attestazioni non si limita alla sola fase di competenza dell'Ufficio, ossia quella di produzione del provvedimento richiesto, ma prevede una serie di attività ulteriori il cui adempimento comporta inevitabilmente una dilatazione dei tempi di conclusione (protocollo, assegnazione, spedizione...).

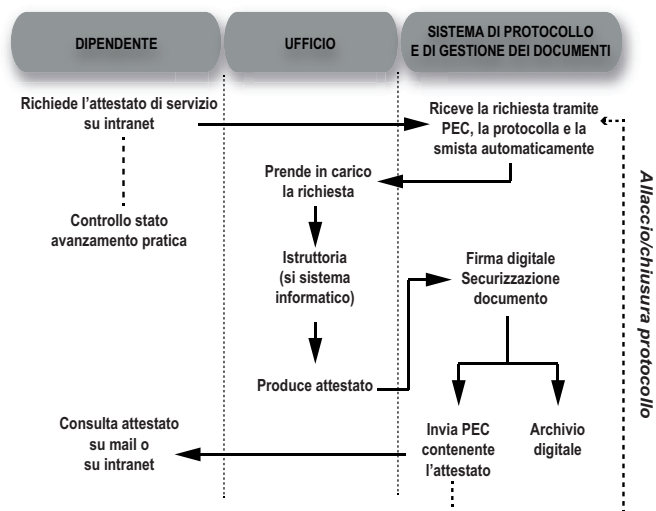


Figura 1. Presentazione schematica del progetto di rilascio delle attestazioni di servizio

La soluzione proposta supera questa problematica, svolgendo in maniera simultanea, grazie al nuovo sistema di protocollo e di gestione dei documenti, alcune operazioni prima cronologicamente distinte, sia in fase di ricezione della richiesta, sia in fase di rilascio dell'attestazione.

In particolare, il progetto accorpa sia le fasi iniziali di inoltro della richiesta da parte dell'interessato, protocollazione in ingresso ed assegnazione all'Ufficio competente, sia quelle finali di securizzazione dell'attestato con apposizione della firma digitale e del "glifo", protocollazione in uscita, invio mediante PEC ed archiviazione digitale.

Un ulteriore vantaggio è rappresentato dalla garanzia di trasparenza dell'azione amministrativa derivante dalla possibilità per l'utente di monitorare in qualsiasi momento lo stato di avanzamento della pratica, grazie ad un sistema di tracciabilità, ed accessibile dal self-service del Sistema Informativo per l'Amministrazione del Personale, disponibile sull'intranet dipartimentale.

Tutta la documentazione così prodotta, inoltre, arricchirà il patrimonio informativo del Dipartimento e sarà archiviata digitalmente per essere, infine, associata al fascicolo informatico del dipendente che oggi si sovrappone a quello cartaceo.

L'altro grande cantiere avviato riguarda la completa revisione del processo di emanazione dei decreti, finalizzata a semplificare la gestione e la fruizione delle informazioni, attraverso l'utilizzo delle nuove opportunità offerte dal sistema di gestione documentale.

La soluzione proposta si caratterizza per l'eliminazione, ove possibile, del documento cartaceo, la definizione di modelli standard da utilizzare per la predisposizione dei decreti, l'introduzione di automatismi che rendano il sistema più affidabile nella qualità del dato, la creazione di correlazioni tra informazioni che attualmente sono svincolate (in particolare tra decreto ed

evento capace di modificare la posizione giuridica registrata sui sistemi di gestione del personale) e, soprattutto, la realizzazione di una funzionalità che consenta di avere a disposizione tutte le principali informazioni che riguardano la storia curriculare e professionale del dipendente, potendo da questa direttamente accedere (mediante link) ai documenti che le certificano.

Nell'attuale processo, l'Ufficio competente all'adozione di ciascun provvedimento emana il decreto in formato cartaceo e provvede all'inserimento a sistema dei relativi estremi, attivando, in tal modo, l'iter di approvazione che passa attraverso la validazione da parte del Dirigente dell'Ufficio, la presa d'atto dell'Ufficio Centrale di Bilancio e l'eventuale registrazione in Corte dei Conti.

Il progetto interviene sulla fase di redazione del provvedimento attraverso una nuova funzionalità che definisce, per ogni tipologia di decreto, uno o più *template* tra i quali scegliere e sui quali apportare le necessarie modifiche; il sistema, a partire dal *template* scelto e dalle informazioni inserite, assegna automaticamente il numero progressivo univoco e predispone il documento elettronico che, in alternativa, può essere stampato per proseguire l'iter di approvazione; al termine del processo il decreto, sotto forma di documento elettronico o di documento cartaceo scansionato, è automaticamente classificato e può essere securizzato prima dell'archiviazione nel fascicolo ottico del dipendente.

Parallelamente le informazioni vengono automaticamente acquisite a stato matricolare (mediante un modello di sintesi predeterminato) e gli eventi registrati nella posizione dinamica propria del modulo Human Resource del Sistema Informativo di gestione del personale (e tramite questo nel sistema per le indagini statistiche la cui base dati che viene, appunto, alimentata da tale sistema).

Tutte le innovazioni tecnologiche sin qui descritte hanno genera-

to conseguenze inevitabili sul versante organizzativo, perché, in assenza di un adeguato e coerente ripensamento dell'organizzazione interna, le nuove tecnologie non possono produrre effetti significativi sulla produttività e sulla qualità dei servizi resi.

A tale scopo, l'Ufficio ha intrapreso un profondo processo di ristrutturazione che fa propri i principi della *lean organization*: l'adozione di questo nuovo modello organizzativo è agevolata dall'utilizzo delle tecnologie informatiche che rendono più facile non soltanto il controllo tra i diversi livelli gerarchici, ma lo stesso autocontrollo da parte del singolo operatore al quale possono essere lasciati margini più elevati di autonomia decisionale. Ciò ha consentito di ridurre il divario tra i diversi livelli gerarchici e di rendere più snelli e tempestivi i processi decisionali e di comunicazione, eliminando i passaggi intermedi divenuti ridondanti.

Anche questa è stata una scommessa importante. Se vogliamo semplificare un processo di per sé complesso, alleggerendo le procedure, abbiamo una sola strada, rendere più complessi i ruoli.

Mi si permetta di dire che questo vale nel caso in cui occorra gestire la complessità. Diverso è il caso di una procedura complicata: la procedura complicata si può sfronare dei passaggi inutili e dei circoli viziosi, ma questo comporta l'aumento dell'efficienza della procedura, non la sua evoluzione qualitativa. Quello che resta dopo questa "ripulitura del superfluo" è la complessità di quel processo. E la complessità non si riduce, ma si gestisce: si può gestire con procedure "complesse" e compiti semplici oppure, se si vuole rendere semplice la procedura, occorre giocare sulla "complessità" dei ruoli, ampliando e qualificando la componente discrezionale. In altri termini, occorre accettare di "delegare le decisioni" utili ad assolvere il compito, passando dal controllo successivo al controllo concomitante (e all'auto-controllo). Questo è un passaggio doloroso, se non ci si

è abituati, sia per il capo che per il collaboratore. Il primo deve rinunciare ad avere il perfetto controllo su ciascun aspetto del lavoro del collaboratore, il secondo deve essere in grado di gestire la responsabilità connessa alla complessità gestita. In realtà, per il capo, in presenza di strutture complesse, il controllo assoluto è illusorio, perché è un controllo sulla procedura che comporta la perdita della visione olistica, unica in grado di permettergli di gestire e cogliere le opportunità di cambiamento, miglioramento, trasformazione.

Eppure non mi sembra ci siano strade alternative: se vogliamo dematerializzare, semplificare, razionalizzare, dobbiamo anche, via via, delegare e puntare sulla professionalizzazione dei collaboratori che sapranno informarci delle eccezioni, delle dimensioni importanti del loro lavoro, ma non dovranno essere rassicurati su quanto sanno fare autonomamente.

Nell'Ufficio, questo processo di trasformazione si è tramutato anche in nuovi ordini di servizio che, oltre a riconoscere le aree di attività assegnate ai dipendenti, hanno voluto chiarire, formalizzare e diffondere i valori fondanti la nuova "filosofia" per tutto il personale.

L'orientamento al risultato, lo spirito di iniziativa, la capacità di lavorare in gruppo, la reciproca condivisione delle informazioni, la flessibilità, intesa come capacità di presidio di più posizioni di lavoro e capacità di espletamento di più attività nella stessa posizione, la standardizzazione delle procedure di lavoro e la loro visibilità e trasparenza sono i fattori che contribuiscono al miglioramento continuo della qualità dei servizi erogati ed alla creazione di un ambiente di lavoro stimolante.

Ovviamente, l'adesione a tali regole di condotta si è immediatamente tradotta in comportamenti concreti che hanno reso possibile la razionalizzazione dei processi lavorativi.

Il flusso di lavoro, ad esempio, è stato razionalizzato, grazie all'utilizzo di archivi "tampone" e di un processo di riproduzione delle pratiche in scadenza che ha permesso di "ripulire" le scrivanie concentrando la lavorazione sulle attività più urgenti e sulle scadenze più prossime. In questo modo, oltre ad essere più efficienti nella lavorazione (è lo scadenziario e non la memoria a scandire le priorità) si è anche tentato di ribadire che "non si lavora per la propria scrivania, ma per l'intera organizzazione".

Le soluzioni appena descritte si sono rivelate di grande utilità non soltanto in fase di erogazione dei servizi, ma anche in sede di controllo dei volumi di attività, dei tempi di evasione delle pratiche, dell'andamento dei flussi di lavoro, dati che, altrimenti, sarebbero stati difficili da monitorare nell'ambito di un'organizzazione tradizionale del lavoro e che, invece, risultano di fondamentale importanza ai fini del controllo di gestione e della valutazione della performance dell'organizzazione prima e del personale poi.

L'esperienza maturata dall'Ufficio nel corso di questi due anni e mezzo mi ha confermato due cose. La prima è che senza la condivisione delle idee con chi opera sulla linea, l'informatizzazione è deleteria e che, quindi, i primi consulenti dell'informatizzazione sono i miei collaboratori. La seconda cosa: non è vero che le persone non vogliono l'innovazione, semplicemente non vogliono l'innovazione inutile, quindi, se voglio operare un processo di riorganizzazione basato sulla digitalizzazione, devo prima provare a convincere chi ci lavora dei vantaggi conseguibili. Se proprio non riesco a convincerli, forse hanno ragione loro e devo ripensare all'utilità della meravigliosa macchina che mi ero immaginato.

Vincenzo Gambetta

La conservazione a lungo termine: tecnologie e soluzioni organizzative

Vincenzo Gambetta

Laureato in Fisica Nucleare, ha trascorso oltre trent'anni in IBM Italia ricoprendo, in Italia e all'estero, incarichi manageriali e professionali. Attualmente è analista di mercato e consulente per la gestione dati, informazioni e documenti presso aziende (fornitrici ed utenti) di medie e grandi dimensioni. Tra i clienti è Assinform per la quale tiene i rapporti con AIPA/CNIPA, il Ministero dell'Economia e delle Finanze e le altre istituzioni coinvolte per garantire la miglior applicabilità delle norme sulla conservazione, sulla fatturazione elettronica e sul documento informatico e firma digitale. In Assinform è, anche, coordinatore dei gruppi di lavoro gestione documentale e outsourcing nonché del centro di competenza per le PMI. È autore delle prime due ricerche sul mercato della gestione elettronica dei documenti in Italia, realizzate per ITER, in collaborazione con le Università Cattoliche di Piacenza (1998) e Milano (2000). È abitualmente relatore in seminari e conferenze e scrive per testate specializzate su temi quali gestione elettronica documenti/contenuti, BPM&A, conservazione, fatturazione elettronica, documento informatico e firma digitale. È direttore contenuti del periodico *iged.it*, specializzato in gestione elettronica dei documenti, e ha la responsabilità scientifica della manifestazione OMAT.

Obiettivo di questo intervento è fornire un quadro dello stato dell'arte delle tecnologie e delle soluzioni organizzative che consentono di realizzare sistemi per la conservazione nel lungo periodo delle informazioni in formato digitale.

Negli ultimi anni¹ il sistema di generazione e trasferimento delle informazioni ha subito radicali trasformazioni vuoi per la facilità con cui le informazioni possono essere generate, trasferite e condivise, vuoi per il conseguente impressionante aumento delle informazioni stesse.

¹ La data all'inizio di questa nuova "era" può essere posizionata a cavallo del 1997, quando la registrazione delle informazioni su supporto magnetico è diventata più economica che non su carta o pellicola fotografica (μ -film).

Questo cambiamento si sta verificando in un arco di tempo molto breve, con conseguente difficoltà a prenderne atto e a mettere in atto le azioni necessarie a gestire e controllare il fenomeno.

Alla facilità di generazione, trasmissione e diffusione ci siamo subito adeguati.

Per quanto concerne le implicazioni normative e giuridiche, anche pressati dall'esigenza di dare certezza al nostro operare, si sta procedendo sempre più spediti ed in modo abbastanza efficace, così pure si sta procedendo per mettere a frutto il potenziale di efficacia, efficienza ed innovazione che il digitale porta con sé in tutte le attività sociali, amministrative e produttive.

La conservazione della memoria digitale è stata, comprensibilmente, un po' "trascurata", essa infatti da un lato non appariva come problema imminente e ..., forse, è il problema più complesso.

Una prima doverosa considerazione: prima di procedere ad una attività di conservazione si deve individuare cosa conservare e quindi, anche cosa "trascurare".

Scartare ciò che non serve è una delle regole auree alla base di un qualunque sistema di archivio; in ambiente digitale ciò è alla base della sua concreta realizzabilità.

Un'idea delle dimensioni del problema si ha pensando che un numero sempre maggiore di organizzazioni dispone oggi di centinaia di Terabyte (1 seguito da dodici zeri), se non addirittura Petabyte (1 seguito da quindici zeri), di informazioni digitali nei propri archivi, ma molte di queste informazioni sono dei file inutili o duplicati, anche di enormi dimensioni (audio, video,...); di tutti questi difficilmente si sa cosa contengano e dove siano; quanto costa tenerli e gestirli, poi, nessuno se lo chiede!

1. Conservare ... per quanto tempo?

Innanzitutto, per quale tempo si deve conservare?

Le risposte alla domanda, di una recente indagine di SNIA², sulle "esigenze temporali di conservazione delle tipologie di dati a ciò interessate" sono riassunte nella Figura 1.

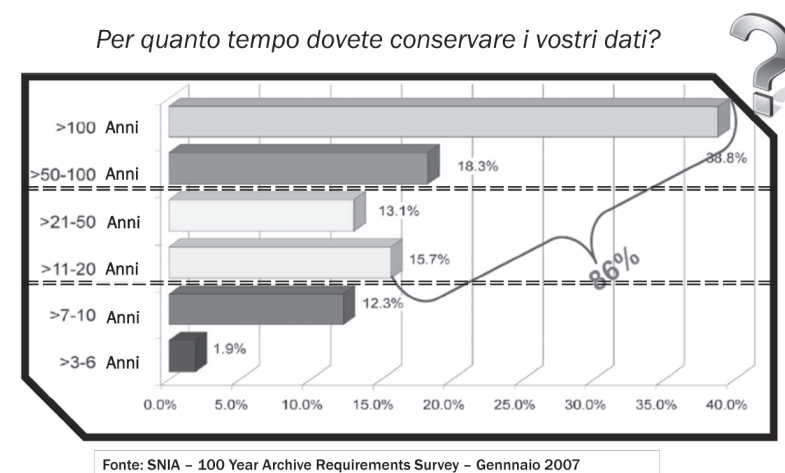


Figura 1. Esigenze temporali di conservazione

Senza entrare in merito ai contenuti si può cominciare a suddividere le esigenze di conservazione almeno in due grandi categorie: quella relativa a tempi di dieci anni al massimo ed il resto.

La prima di queste due categorie, quella più rilevante in termini di volumi, raccoglie tutti i documenti di tipo amministrativo e commerciale la cui conservazione è regolata da precise norme.

Oltre i dieci anni è il tipo di informazione contenuta che determina i tempi di conservazione; tempi che possono arrivare, in

² Storage Networking Industry Association.

linea di principio, a prevedere la conservazione “per sempre” dei documenti coinvolti (ad esempio: documentazione istituzionale che “racconta” la storia e l’evoluzione di importanti organizzazioni o amministrazioni e degli Stati).

Appare evidente che è questa seconda categoria di dati, informazioni, o documenti quella che merita la maggior attenzione, proprio a causa del “tempo” coinvolto, nel corso del quale comportamenti e tecnologie si possono “modificare” in modo difficilmente prevedibile, ma di cui si deve, inevitabilmente, tener conto.

2. La conservazione della memoria digitale in Italia

Nel nostro Paese la conservazione digitale comincia a prendere concretamente piede nel 2004 con la pubblicazione della Deliberazione CNIPA n. 11 del 19 febbraio 2004 (che ha introdotto il termine conservazione sostitutiva³) e del Decreto del Ministro dell’Economia e delle Finanze del 23 gennaio 2004, con le successive circolari e risoluzioni dell’Agenzia delle entrate, che hanno delineato un quadro realisticamente concreto per procedere alla conservazione dei documenti rilevanti ai fini tributari.

Il grosso merito di queste norme è stato quello di far prendere coscienza dell’imprescindibile necessità di affrontare e trovare una soluzione pratica ed efficace alla conservazione digitale.

Dopo più di 7 anni di “onorato servizio” la conservazione sostitutiva cederà a breve il posto a nuove e più moderne norme sulla conservazione di documenti digitali.

Il numero dei progetti di conservazione sostitutiva, alla data, è

³ Questo termine, di per se improprio, è molto probabilmente il risultato di una “fusione” tra due concetti distinti: la Conservazione di Documenti Digitali (Informatici, secondo la terminologia adottata dalle norme) e la Conservazione di Documenti in Formato Digitale che sostituiscono documenti originali cartacei od informatici (con modifica di formato). Essendo entrato nella terminologia corrente non si disdegnerà di usarlo.

stato valutato dall’Osservatorio Fatturazione Elettronica e Dematerializzazione del Politecnico di Milano intorno a 4.000 (con una crescita del 56% circa rispetto all’anno precedente).

Le esigenze di conservazione della stragrande maggioranza dei documenti coinvolti, inoltre, rientrano nei termini legali e, quindi, “solo” per un arco di tempo di dieci anni, o poco più: essi sono nel 73% dei casi fatture attive, nel 28% fatture passive e nel 60% libri e registri.

Se, poi, si guarda alla dimensione aziendale, una buona metà di queste sono micro-imprese (con meno di 10 dipendenti).

3. I principi della conservazione della memoria digitale

Conservare documenti digitali per un arco di tempo sufficientemente breve, a parte il rispetto di specifiche normative (vedi documenti fiscalmente rilevanti), non presenta particolari difficoltà.

Conservare il digitale nel lungo periodo è, invece, un problema certamente molto complesso.

In tutto il mondo si stanno conducendo importanti studi e progetti per individuare come riuscire a conservare per molti decenni, se non per secoli, l’ingente quantità di differenti tipologie di informazioni digitali che stiamo producendo.

Si tratta di sistemi che hanno l’obiettivo di garantire la sicurezza e l’autenticità delle informazioni digitali nonché di rendervi possibile l’accesso in un futuro, anche remoto, consentendo di mantenerne la comprensione e le modalità d’impiego dei dati che contengono anche quando le attuali tecnologie impiegate per l’hardware, i sistemi operativi, i sistemi di data management e gli applicativi potrebbero non essere più disponibili.

Questi obiettivi si possono ottenere agendo principalmente su:

1. l'integrità delle registrazioni, ossia rendere possibile, un domani, indipendentemente dalle tecnologie disponibili, il recupero della sequenza di bit originariamente archiviata;
2. il formato, in cui il documento/informazione è registrato, deve consentire di interpretare la stringa di bit recuperata e offrire a chi la consulta lo stesso "documento" così come è stato creato;
3. la capacità di assicurare l'integrità e l'autenticità del documento, nel tempo. Opportune combinazioni di tecniche di protezione (esempio: la firma digitale) e di buone pratiche di controllo e custodia (esempio: l'ininterrotta custodia) consentono di avere la ragionevole certezza che le informazioni che si andranno ad esaminare saranno affidabili;
4. una corretta scelta e gestione dei metadati. In ambiente digitale si rafforza l'esigenza di definire quali sono i metadati da conservare per comprendere appieno il contesto cui l'informazione si riferisce, a quale altre informazioni è correlata ed in che modo.
5. Non esiste una risorsa informativa digitale senza che ad essa sia associata una sequenza di bit con le informazioni su ciò che è, che descrive e che rappresenta.
6. Queste coppie dati-metadati sono indivisibili, anche se piuttosto aperte: la risorsa originaria nel corso della sua (lunga) vita è infatti soggetta ad una serie importante di interventi, di autenticazione, elaborazione, verifica, trasferimento e accesso, effettuati da vari soggetti, mutevoli nel tempo, ma dotati dei diritti necessari.

4. Il modello OAIS

Uno dei modelli di riferimento per un sistema di Conservazione Digitale è OAIS – Open Archival Information System (ISO 14721:2003), concepito per essere adottato in un qualunque contesto di conservazione digitale (archivistico, bibliotecario o altro).

Un importante concetto insito in tale modello è quello di "comunità di riferimento" (è necessario definirne caratteristiche, natura ed esigenze): può sembrare banale, ma quando si porta qualcosa in conservazione lo si fa a beneficio di soggetti ben identificabili dotati della capacità di comprendere ed utilizzare l'informazione conservata.

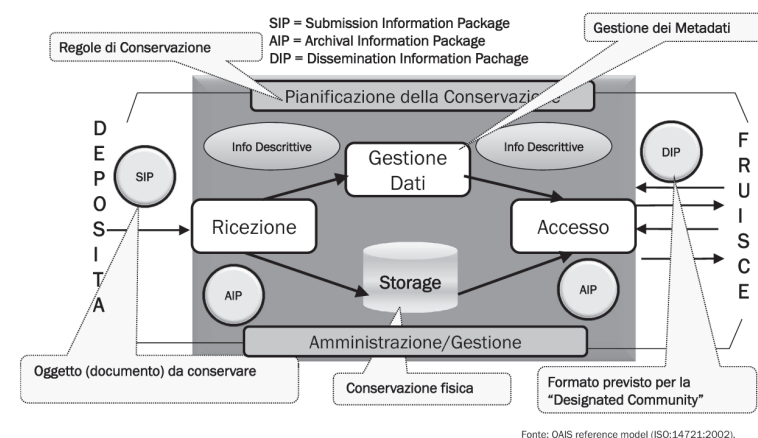


Figura 2. Il modello OAIS

Le componenti funzionali di OAIS sono: la ricezione dei dati, la loro archiviazione, la loro gestione, l'accesso ai dati conservati, l'amministrazione dell'archivio e la pianificazione della conservazione.

L'ambiente applicativo definito in OAIS è composto di quattro entità: i produttori, gli utenti, il management (la gestione dei dati e la pianificazione della conservazione) e l'archivio.

Il produttore deposita le risorse in OAIS affinché siano conservate, in base ad un accordo formale che contiene le regole per questa operazione. L'utente interagisce con l'archivio per ricercare ed acquisire le risorse. Il management si occupa delle politiche complessive del sistema e ne determina lo sviluppo.

L'archivio contiene l'insieme delle risorse informative.

OAIS descrive, anche, un modello di organizzazione dei dati basato su "Pacchetti Informativi"⁴ composti da dati e dai metadati necessari per interpretarli correttamente.

Il processo gestionale e di conservazione deve essere applicato quindi tanto ai dati quanto ai metadati.

Ogni scambio di informazione da, per e all'interno dell'archivio avviene attraverso essi.

I pacchetti informativi sono di tre tipi:

- il SIP (Submission Information Package), utilizzato nella fase di immissione dei dati e generato a cura dal produttore;
- l'AIP (Archival Information Package), destinato alla conservazione a lungo termine;
- il DIP (Dissemination Information Package), utilizzato per il trasferimento all'utente in base ad una richiesta di accesso.

5. I formati

Il "formato" descrive l'organizzazione dei bit che costituiscono l'oggetto (documento) e l'informazione in esso contenuta; esso contiene anche i dati necessari (metadati) ad interpretare correttamente il suo contenuto.

Esistono oltre 1.500 formati (individuati generalmente dalla "estensione" del file utilizzato per memorizzarli); per almeno un terzo di questi non è nota la descrizione!

⁴ Information Packages (IP).

Essi possono riguardare testi/documenti (doc, docx, xml, html, pdf,...), immagini (gif, jpg, bmp, tif, cgm, eps, svg, ...), suoni (mp3, wav, ...), filmati (mpg, mpeg, avi, wmv,...), oggetti eseguibili (exe, ...), strumenti di calcolo (xls, mdb, ...), oggetti risultato di operazioni di compressione (zip, rar, ...), altre strutture di dati quali gli output di strumentazione di laboratorio o le firme elettroniche (p7m, p7f, ...), email e tanto altro ancora.

Un formato può essere in grado di contenerne altri (esempio: un formato di gestione testi che incapsula immagini o grafici).

I formati, poi, possono essere "standard" o "proprietary" (noti solo da chi li ha ideati e utilizzati nelle proprie applicazioni), oppure "preferenziali" (quando il loro impiego è caratteristico di un'applicazione) o compatibili (quando una o più applicazioni li riconoscono oltre al/ai formati preferenziale/i).

Importanti caratteristiche utili a valutare un formato sono:

- la diffusione - il numero di persone ed organizzazioni che li adotta;
- la portabilità - il numero di applicazioni e/o piattaforme in grado di riconoscerlo;
- le funzionalità a disposizione dell'utente per elaborare l'informazione e collegarla ad altre;
- la capacità di occupare il minor spazio possibile in fase di memorizzazione;
- la possibilità di gestire il maggior numero possibile di metadati;
- la disponibilità di visualizzatori che consentono la fruibilità delle informazioni.

Nella fase di gestione del documento, l'utente deve avere a disposizione la massima flessibilità in termini di formati e funzionalità disponibili. Gli unici limiti ai formati, e ai relativi programmi

di gestione, possono essere quelli imposti dall'organizzazione cui appartiene per esigenze di interscambio, di interoperabilità od operative.

Sostanzialmente diversi sono gli elementi di valutazione di un formato se l'oggetto che descrive deve essere utilizzato per conservarlo nel lungo periodo: il formato deve, infatti, consentirne il "riconoscimento" ed il corretto impiego nel tempo ed agevolarne l'inalterabilità.

In sintesi, le caratteristiche che contribuiscono a qualificare un formato per tale utilizzo sono:

- l'immodificabilità non deve consentire di apportare modifiche al contenuto (a qualunque livello, struttura e modalità di visualizzazione comprese);
- il mantenimento della fedeltà di presentazione del contenuto non significa semplicemente conservare nel tempo la struttura del documento, ma anche i "font" e tutte le altre caratteristiche utili alla sua completa comprensione;
- non contenere riferimenti ad altre informazioni o documenti (ad esempio link ipertestuali) non sotto il controllo della stessa "unità di informazione" o documento;
- corrispondere fedelmente ad uno standard interamente descritto e le cui specifiche siano state rese di dominio pubblico senza limitazioni.

Logica conseguenza delle diverse caratteristiche dei due tipi di formato appena descritte è la necessità, al momento in cui un documento diviene oggetto da portare in "conservazione", di procedere ad un processo di conversione del formato da "operativo" a quello individuato per la sua conservazione.

Alla data sono pochi i formati che soddisfano i requisiti illustrati o che, con le dovute precauzioni, possono essere impiegati in processi di conservazione digitale. Essi sono:

- il PDF/A-1 (ISO 19005-1); esso può anche disporre di uno "strato" XML (in grado di trasportare dati strutturati e metadati) ed ha la possibilità di "inglobare" un'eventuale Firma Digitale;
- il formato immagine (raster) TIFF, in versione non compressa o compressa senza perdita di informazione. Di questo formato vi sono parecchie versioni, alcune delle quali proprietarie, ma in genere le specifiche sono pubbliche e non soggette ad alcuna forma di limitazione;
- sono formati molto utilizzati per la conversione in digitale di documenti cartacei;
- il loro impiego, se attuano una forma di compressione, va valutato attentamente;
- JPEG 2000 (ISO/IEC 15444-1); questo formato può utilizzare la compressione senza perdita di informazione e consente di associare metadati ad un'immagine. Il suo limite è che ha una diffusione abbastanza limitata.

Non sono, però da trascurare formati quali Open XML (ISO/IEC 29500). È questo un formato indirizzato all'elaborazione di testi, presentazioni e fogli di calcolo. Tra le sue funzionalità, oltre alla possibilità offerte dall'XML, può includere i font utilizzati e gestire i metadati. Pur essendo molto recente comincia ad essere adottato da parte di vari prodotti e piattaforme.

Oppure i formati TXT, purché si abbia l'accortezza di specificare la Codifica del Carattere (Character Encoding) adottata.

In questi casi di formati "in chiaro", dando per scontato che siano stati eliminati - se presenti - durante la fase di creazione dei documenti - macro e/o codici eseguibili, va tenuto presente che essi sono e saranno sempre facilmente modificabili: se il sistema di conservazione, pertanto, non prevede opportuni funzionalità che garantiscano l'immodificabilità dei documenti in conserva-

zione si dovrà provvedere a renderli tali con opportune tecniche quali quelle della firma digitale. Quanto sinteticamente illustrato ha per forza di cose valenza generale.

Vi sono particolari (che non significa poche) applicazioni (fatturazione elettronica, applicazioni finanziarie, ...) o campi di applicazioni (sanità, ...) che prevedono specifici formati per la documentazione che li riguarda. I principi appena illustrati possono essere utile guida per valutare i formati da utilizzare per portare i documenti coinvolti in conservazione digitale ed individuare le precauzioni da adottare.

6. Le tecniche e le strategie relative allo Storage

Per la conservazione nel lungo periodo è necessario impiegare prodotti e tecnologie professionali, anche se per la conservazione “a norma” si è diffuso nel tempo l’uso di tecnologie “consumer”, come CD e DVD, quali surrogati di quelle professionali più costose.

Le soluzioni professionali, sono realizzate mantenere le registrazioni nel tempo, mentre i supporti quali CD e DVD, sono stati pensati per applicazioni d’intrattenimento o per distribuire informazioni a costi ridotti e, comunque, con esigenze di durata di gran lunga inferiori.

Considerando, in conservazione, l’adozione di supporti non professionali è limitato e, nella maggior parte dei casi, coinvolge organizzazioni di piccole dimensioni, volumi ridotti e tempi di conservazione limitati, non si ritiene si debba intervenire su quanto fin ora realizzato con supporti non professionali. Anche per analoghe realizzazioni future l’adozione di supporti non professionali possa essere accettata, se accompagnata da opportune misure di prudenza.

Le tecnologie professionali sono oggi divisibili in due categorie: i dischi magnetici e i nastri magnetici; entrambi sono general-

mente utilizzati all’interno di sottosistemi più complessi, spesso dotati di funzionalità avanzate per la conservazione e per il recupero dei dati gestiti.

I sottosistemi a dischi magnetici prevedono la conservazione dei dati su supporti non rimovibili; i sottosistemi a Nastri Magnetici hanno, invece, supporti rimovibili. Di dischi magnetici ne esistono per tutte le esigenze: a livello di prestazioni, costi, capacità, scalabilità, affidabilità, consumo, modalità di connessione,

Dal punto di vista della durata ciò che ha senso è considerare il ciclo di vita economico della tecnologia: nel caso di dischi magnetici va dai 3 ai 5 anni, mentre, per i nastri, è di circa 5-10 anni per le cartucce e 20 - 30 anni per le librerie.

Non è questo, però, ancorché importante, l’unico parametro cui fare riferimento per individuare la tecnologia più adatta alle proprie esigenze di conservazione.

Le informazioni in formato digitale sono per loro natura immateriali e si affidano per la loro “sopravvivenza” ai dispositivi fisici sui quali sono registrati.

Una prima distinzione da fare è tra la protezione contro la perdita accidentale delle registrazioni nel periodo in cui le informazioni sono “attuali” e quella da attuare durante la conservazione delle registrazioni nel lungo periodo.

È abbastanza intuitivo che le tecniche e le strategie da utilizzare nel secondo caso devono comprendere, per forza di cose, anche quelle che servono nel corso della prima.

La prima “precauzione” cui viene spontaneo pensare, dato che i dischi magnetici sono quelli maggiormente impiegati (in particolare nelle attività correnti), è una forma diretta di auto-protezione rappresentata, ad esempio, dalle tecnologie RAID (Redundant Array of Independent Disks) o dalle loro evoluzioni.

Questi sistemi sono in grado di bilanciare a vari livelli due importanti esigenze: la protezione contro la perdita di dati dovuta a guasti e le prestazioni del sistema intese come velocità di accesso alle informazioni.

Quando si progetta un sistema per la conservazione nel lungo periodo, si premierà la tecnologia che privilegia la protezione contro la perdita delle informazioni (elevata ridondanza).

Si raccomanda, altresì, la presenza di dischi/nodi di riserva che possono essere utilizzati dalla unità per ricreare in modo automatico i livelli di ridondanza richiesti. Ciò è ancor più vero per quelle unità che conservano informazioni di controllo e di accesso alle registrazioni (metadati).

Altra caratteristica importante, a garanzia della corretta effettuazione delle registrazioni, è la verifica automatica di quanto registrato, ottenibile solo con sistemi professionali.

Si consiglia, inoltre, di prevedere procedure periodiche di rilettura/verifica dei dati in essi contenuti. Sono in commercio sistemi che verificano ciclicamente i dati registrati, altri adottano tecniche di memorizzazione che associano al dato un'ulteriore informazione di controllo che garantisce l'integrità del dato nel tempo.

Una delle più evidenti caratteristiche delle informazioni in formato digitale, poi, è proprio la facilità con cui esse possono essere duplicate riproducendo altrettanti "originali". Ecco perché le più diffuse strategie di protezione sono di fatto coincidenti con opportune strategie di replica (le stesse informazioni sono mantenute aggiornate - replicate - in sistemi e/o in siti differenti) o copia.

Le procedure di protezione dati devono essere documentate e sottoposte a collaudi periodici (tipicamente ogni anno) per verificare l'efficacia dei processi di ripristino e per affinare la formazione del personale operativo.

Le tecnologie di memoria digitale sono soggette a continui miglioramenti che puntano alla riduzione dei costi e ad aumentare l'affidabilità e le prestazioni. Ciò comporta un processo di obsolescenza dei dispositivi di memoria digitale e la conseguente necessità di trasferire i dati su nuove tecnologie.

Un sistema di conservazione digitale deve, quindi, dotarsi di opportune procedure che consentano l'indipendenza nel tempo dalle tecnologie di memoria mediante un piano di migrazione controllata su nuovi dispositivi. Il processo di riversamento periodico deve diventare parte delle procedure di gestione del sistema di conservazione, deve essere ben documentato e devono essere messi in atto opportune procedure di verifica del corretto completamento di tali operazioni.

Particolare attenzione deve essere posta all'eventuale esigenza di corretto aggiornamento delle informazioni di controllo (metadati) per garantire l'accesso ai dati sui nuovi dispositivi.

In base a quanto brevemente descritto, si delineano ulteriori compiti in capo al Responsabile della Conservazione:

- documentare ed aggiornare periodicamente le procedure di protezione dati anche a fronte di eventi disastrosi;
- verificare periodicamente, mediante controlli a campione, la validità dei dati registrati;
- verificare periodicamente mediante prove (almeno con cadenza annuale) la capacità di ripristino dei dati coinvolgendo il personale addetto;
- verificare periodicamente (almeno ogni 3 anni) l'obsolescenza tecnologica dei dispositivi utilizzati, dei formati e del software di accesso ai dati al fine di pianificarne le attività di riversamento;
- documentare l'esito delle prove e delle eventuali azioni per la correzione e/o miglioramento del processo.

Andrea Lisi

Guida alla migliore scelta del responsabile “in outsourcing” per la conservazione digitale dei documenti

Avvocato esperto in ICT Law, Presidente ANORC – www.anorc.it - titolare del Digital&Law Department Studio Legale Lisi – www.studiolegalelisi.it)¹.

1. Il responsabile della conservazione: profili generali

Il concreto sviluppo di un sistema di conservazione digitale dei documenti si incentra nella figura del responsabile della conservazione. La nomina di tale soggetto assume particolare importanza per il processo di conservazione e va necessariamente valutata alla luce dei compiti e delle responsabilità che la normativa prevede in maniera specifica per questa delicata figura.

Il “responsabile del procedimento di conservazione sostitutiva” ha in carico il processo di conservazione e di esibizione della documentazione che si è deciso di conservare a norma. Egli, dunque, ha il compito principale di attestare il corretto svolgimento del processo di conservazione apponendo, come se fosse un definitivo e autorevole sigillo, la propria firma digitale e un riferimento temporale sul documento conservato o, meglio, sul “lotto” di documenti (o impronte di documenti) da conservare. Inoltre, nell’ambito della gestione dell’intero iter di conservazione digitale, il responsabile si rende garante della corretta tenuta dell’archivio secondo principi documentati di sicurezza, attraverso l’adozione di procedure di tracciabilità tali da garantire la corretta conservazione, l’accessibilità e l’esibizione dei documenti.

¹ Per la stesura del presente saggio ci si è avvalsi della proficua collaborazione dell’avv. Francesca Giannuzzi.

Si può, quindi, affermare che il vero obiettivo del responsabile del sistema di conservazione digitale dei documenti sia quello di definire e realizzare, attraverso un'opportuna organizzazione delle attività e mediante idonee procedure informatiche, il processo per il trattamento della documentazione soggetta a conservazione sostitutiva.

Va da sé, dunque, ogni riferimento all'importanza e strategicità che tale figura assume per l'intero processo di conservazione digitale dei documenti², caratteristiche queste che vengono maggiormente alla luce qui di seguito, allorquando si analizzano, nello specifico, le sue funzioni e le competenze richieste alla luce della tipologia di documenti da conservare.

Da ciò l'attenzione che necessariamente e incontestabilmente deve essere riposta nella fase di scelta del responsabile del processo di conservazione da parte dell'azienda/pubblica amministrazione interessata.

2. Compiti e responsabilità

La Deliberazione CNIPA n. 11/2004, normativa tecnica attualmente in vigore, dedica al responsabile della conservazione l'intero art. 5, attribuendogli precisi compiti e specifiche responsabilità³.

² La grande attenzione che viene riposta su tale figura è confermata, tra l'altro, dalla pubblicazione da parte di DigitPA delle nuove "Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 44 e 44 bis del Codice", la cui bozza è aperta alla consultazione pubblica dallo scorso 5 agosto 2011.

³ Più in dettaglio, l'art. 5 comma 1 della Deliberazione afferma che "il responsabile del procedimento di conservazione sostitutiva:

a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;

b) archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:

- descrizione del contenuto dell'insieme dei documenti;

Sulla base di quanto disposto dalla normativa, i compiti del responsabile della conservazione possono essere sintetizzati in:

- compiti organizzativi, ossia definire le caratteristiche e i requisiti del sistema di conservazione, definire il manuale operativo della conservazione⁴, partecipare a incontri e seminari formativi dedicati alle procedure di conservazione digitale, definire le procedure informatiche, organizzative e di sicurezza inerenti al processo di conservazione, etc.;
- compiti di registrazione, cioè garantire la corretta archiviazione delle informazioni caratterizzanti ciascun supporto di memorizzazione, assicurandone la disponibilità in caso di richiesta, descrivere in dettaglio le attività del processo di conservazione (gestione ordinaria, gestione delle anomalie, ispezioni e verifiche), i documenti conservati, le figure coinvolte (ruoli, deleghe, responsabilità, formazione) e gli strumenti utilizzati, etc.;

-
- estremi identificativi del responsabile della conservazione;
 - estremi identificativi delle persone eventualmente delegate dal responsabile della Conservazione, con l'indicazione dei compiti alle stesse assegnati;
 - indicazione delle copie di sicurezza.
- c) mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;
- d) verifica la corretta funzionalità del sistema e dei programmi in gestione;
- e) adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
- f) richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- g) definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- h) verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti".

⁴ Il manuale della conservazione sostitutiva è un documento in cui sono descritti tutti i dettagli dell'organizzazione e delle procedure operative, informatiche, di sicurezza, etc. del processo di conservazione.

- compiti di manutenzione e controllo, ovvero effettuare specifici controlli sui sistemi software e sui supporti hardware utilizzati per la conservazione, conservare in archivio le differenti versioni e release dei programmi adottati per la conservazione a norma, aggiornare i certificati di firma, verificare la validità delle marche temporali, verificare periodicamente la leggibilità dei documenti, provvedendone, se necessario, al riversamento, etc.;
- compiti operativi, cioè supervisionare l'intero processo di archiviazione e conservazione sostitutiva, verificare la effettiva leggibilità dei documenti prima dell'apposizione della firma digitale e della (eventuale) marca temporale e la leggibilità dei supporti contenenti i documenti alla fine del processo di conservazione, ossia prima della loro archiviazione in luogo sicuro, tenere aggiornato il manuale operativo della conservazione, etc.;
- compiti per la protezione dei dati e delle procedure informatiche, ovvero garantire tutte le misure necessarie per la sicurezza fisica, logica e ambientale dei dati e del sistema preposto alla loro conservazione (comprensivo della copie di sicurezza dei supporti di memorizzazione), garantire la tutela della privacy attraverso un trattamento a norma di dati e informazioni personali, etc.;
- compiti di assistenza/ispezione, ossia garantire l'adeguato supporto ai vari delegati che svolgono le attività di conservazione, ispezionare i luoghi in cui vengono eseguite le attività di registrazione delle informazioni digitali e di conservazione a garanzia della validità giuridica e fiscale del processo, per non incorrere nelle sanzioni previste per mancata osservanza, etc.;
- compiti di natura fiscale (o relativi alla specifica tipologia di documenti da conservare), ovvero fornire l'assistenza in tutti i casi in cui sia necessario il suo intervento, sia per la verifica – a campione – della validità dei supporti, sia per eventuali aggiornamenti riguardanti la regolamentazione fiscale (e/o

giuridica) rilevante, sia nel caso di controlli da parte delle autorità di vigilanza⁵.

3. Il responsabile della conservazione digitale di documentazione sanitaria

Se le competenze generalmente richieste al responsabile della conservazione sono altamente specialistiche non solo sotto il profilo normativo, ma anche tecnico-organizzativo proprio per la delicata e importante tipologia di mansioni che normalmente è chiamato a svolgere, il livello di tali competenze aumenta e le stesse si diversificano e settorializzano nel caso in cui ad essere conservate digitalmente siano le cartelle cliniche o, comunque, la documentazione contenente dati sanitari. Pertanto, le cautele e le accortezze prescritte in via generale dall'art. 51 comma 2 del Codice dell'amministrazione digitale (D. Lgs. 82/2005, qui di seguito più brevemente CAD)⁶ assumono, in questo ambito, un significato ancora più denso e pregnante. Invero, la natura stessa di tale tipo di documentazione impone maggiori cautele e accortezze nella sua conservazione: la valenza giuridica, ad esempio, delle cartelle cliniche, costituenti veri e propri atti pubblici certificativi muniti di fede privilegiata, necessita di procedimenti di conservazione che garantiscano l'immodificabilità e l'irretrattabilità⁷ del loro contenuto. Ma vi è più: i dati contenuti nella

⁵ Altri compiti sono individuati dal DMEF 23 gennaio 2004 relativamente alla conservazione dei documenti fiscalmente rilevanti in capo al responsabile della conservazione:

a) nella fase di apposizione di firma digitale e marca temporale, dovrà scegliere se operare sull'insieme dei documenti, sull'unica impronta di essi oppure su più impronte che rappresentano i singoli documenti o insiemi di essi (art. 3, comma 2);

b) se appositamente designato, garantisce l'invio dell'impronta dell'archivio oggetto di conservazione alle competenti agenzie fiscali (art. 5 comma 1 DM 23 gennaio 2004).

⁶ L'art. 51, comma 2, prescrive che “I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta”.

⁷ Cfr. Telesio Perfetti, “La dematerializzazione dei documenti sanitari”, pubblicato su www.filodiritto.com.

documentazione sanitaria e clinica sono a tutti gli effetti dei dati c.d. “supersensibili”, in quanto idonei a rivelare lo stato di salute, gli orientamenti sessuali nonché i dati genetici dei pazienti. Da ciò, l’inevitabile interessamento della normativa sulla privacy con particolare riferimento al trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche⁸. Il CAD, infatti, all’art. 51 comma 1, prevede delle specifiche regole tecniche da adottarsi ai sensi del successivo art. 71, a tutela dell’esattezza, disponibilità, accessibilità ma, soprattutto, per quel che qui rileva, dell’integrità e riservatezza dei dati, dei sistemi e delle infrastrutture.

Per gli stessi motivi anche il CAD, nella sua nuova formulazione, così come modificato dal D. Lgs. n. 235/2010, prevede espressamente la necessità di un lavoro congiunto tra il responsabile della conservazione sostitutiva e il responsabile del trattamento dei dati personali nella gestione del relativo sistema di conservazione⁹. Nel caso della conservazione della documentazione sanitaria, poi, il binomio “conservazione-privacy” appare assolutamente indissolubile. Infatti, il Garante Privacy si è occupato più volte della regolamentazione della dematerializzazione della documentazione sanitaria attraverso una serie di provvedimenti¹⁰. Più precisamente, sono state previste delle misure di sicurezza da adottare per la gestione della documentazione clinica testuale e iconografica ottenuta direttamente in formato digitale, e sono state impartite delle istruzioni tecniche specifiche

⁸ Non solo quindi assume rilevanza il Codice Privacy (D. Lgs. 196/2003), ma anche i successivi provvedimenti del Garante Privacy nonché la normativa comunitaria.

⁹ L’art. 44, comma 1-bis, del CAD prevede, inoltre, che il lavoro congiunto debba sussistere anche con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

¹⁰ I provvedimenti del Garante per la protezione dei dati personali relativi alla conservazione digitale della documentazione sanitaria sono: Provvedimento del 26 novembre 2009, “Dematerializzazione della documentazione clinica”; Provvedimento del 19 novembre 2009 contenente le Linee guida in tema di referti on-line; le Linee Guida 16 luglio 2009 disciplinanti il Fascicolo Sanitario Elettronico e il dossier sanitario.

per tutti i responsabili della conservazione che si trovino a dover gestire documenti contenenti dati sanitari. Ecco, pertanto, che la scelta del responsabile della conservazione sostitutiva della documentazione sanitaria risulta di fondamentale importanza, atteso sia il compito delicato che viene allo stesso affidato, sia le implicazioni e le responsabilità che da tale nomina derivano.

4. La gestione in outsourcing del sistema di conservazione

Il sistema di conservazione potrà essere affidato a una figura interna dell’ente (dirigente, legale rappresentante, dipendente), oppure a una persona fisica o giuridica esterna all’organizzazione come, ad esempio, una società informatica altamente specializzata¹¹.

Anche nel caso in cui sia nominata una figura interna come responsabile del processo di conservazione, è sua possibile facoltà direttamente delegare parte dei propri compiti/responsabilità ad altri soggetti interni o esterni, così come espressamente previsto dalla Deliberazione del CNIPA 11/2004¹². Una particolare ocularità dovrà sempre contraddistinguere la fase di scelta del responsabile della conservazione¹³, indipendentemente dal fatto che questo soggetto venga scelto all’interno dell’azienda, o all’esterno della stessa, originariamente o in virtù di delega.

¹¹ Rimane sempre necessario prevedere un responsabile interno all’azienda o PA che abbia lo specifico compito di supervisionare l’attività sviluppata dal responsabile esterno a cui è stato affidato l’intero processo di conservazione digitale.

¹² Art. 5, commi 2 e 3 della citata Delibera CNIPA 11/2004: “il responsabile del procedimento di conservazione sostitutiva può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad essa delegate. Il procedimento di conservazione sostitutiva può essere affidato, in tutto o in parte, ad altri soggetti, pubblici o privati, i quali sono tenuti ad osservare quanto previsto dalla presente deliberazione”.

¹³ Numerosi sono infatti i profili di responsabilità non solo per colui che viene nominato Responsabile, ma anche per colui che lo sceglie, in quanto, nel caso di selezione sbagliata, si possono profilare due tipi di responsabilità: per “culpa in eligendo”, se il responsabile è palesemente inaffidabile, e per “culpa in vigilando”, se il titolare non ha vigilato sul corretto trattamento che il responsabile designato ha fatto dei dati personali forniti.

4.1 Le modalità di conferimento all'esterno dell'incarico

4.1.1 La delega

Considerato il numero e la complessità dei compiti previsti dalla normativa, è frequente che il responsabile della conservazione deleghi ad altri soggetti parte di tali compiti, lasciando per sé una funzione di controllo e di coordinamento generale.

È auspicabile che la delega sia conferita a persone che, per competenza ed esperienza, siano in grado di garantire la corretta esecuzione del lavoro. In ogni caso, si ritiene comunque assolutamente necessario il conferimento dell'incarico a mezzo di atto formale di nomina con relativa accettazione. È buona norma, infatti, delegare processi e responsabilità nell'ambito di specifici accordi contrattuali, aggiungendo sempre le opportune lettere di delega. La lettera di delega rappresenta un atto formale e giuridico con il quale si trasferiscono, in maniera più specifica di quanto può avvenire in un contratto (al quale deve essere comunque e sempre correlata), i doveri e le responsabilità in capo al delegato.

4.1.2 Tipi di delega e tipi di rapporti delegante/delegato

La lettera di delega può avere diverse forme di stesura e tale modalità di redazione dipende strettamente dal rapporto tra delegante e delegato.

Il rapporto può, infatti, essere:

- diretto, quando il delegante incarica direttamente il delegato;
- oppure indiretto, ossia nel caso in cui il delegante incarica un delegato che, a sua volta, delega ad un terzo il processo (cosiddetta “delega a tre”)¹⁴.

¹⁴ Quest'ultimo caso è piuttosto frequente. Capita, infatti, molto spesso che terzi intermediari (normalmente studi professionali o società non specializzate nella conservazione) vengano incaricati dalle aziende a svolgere il ruolo di responsabile della conservazione ma, mancando a questi la possibilità di realizzare integralmente il processo, essi lo deleghino, a loro volta,

La normativa permette tale ultimo tipo di delega: l'importante è che il delegante venga sempre messo a conoscenza del fatto che il delegato ha, a sua volta, delegato il processo stesso o parte di esso e a chi lo ha delegato, e che si citino tutti i termini della normativa su cui la delega si basa, nonché tutti i diversi passaggi contrattuali.

4.2 L'outsourcing

L'art. 5 della delibera CNIPA, al comma 3, ammette la possibilità che il procedimento di conservazione sostitutiva venga affidato, totalmente o parzialmente, ad altri soggetti, pubblici o privati, i quali saranno tenuti ad osservare quanto previsto dalla medesima deliberazione.

Tale articolo va oltre la possibilità, già esaminata, di delegare all'esterno alcuni o tutti gli oneri gravanti sul responsabile, in quanto ammette che l'ente/azienda, in tal caso, demands l'intero processo di conservazione a soggetti diversi, con tutto ciò che ne deriva in termini di attribuzione diretta degli eventuali danni derivanti dalla non corretta gestione del processo di conservazione¹⁵.

I passi che l'azienda (o la PA) dovrà seguire prima di procedere alla scelta del partner sono:

1. effettuare una valutazione di convenienza, in termini di costi/ benefici, per stabilire se la decisione di esternalizzare il processo sia effettivamente conveniente. Si deve tener presente, infatti, che in molti casi tale scelta consente di evitare che compiti prettamente tecnici, quali quelli propri del responsabile della conservazione, vengano eseguiti da soggetti che, seppur in posizione di apice all'interno dell'unità orga-

parzialmente o totalmente, ad *outsourcer* specializzati.

¹⁵ Qualora non rispetti le regole previste dal decreto ministeriale 23 gennaio 2004 applicabile ai documenti fiscali e nell'articolo 5 della deliberazione 19 febbraio 2004, sarà, infatti, tenuto a risarcire tutti i danni che sono derivati dalle sue inadempienze.

nizzativa di cui fanno parte (si pensi, ad esempio, ai Direttori Sanitari o ai Responsabili dell'UO, responsabili fino al momento dell'archiviazione dei documenti), raramente hanno le competenze specialistiche necessarie per far fronte a tali incombenze;

2. realizzare una corretta analisi di mercato che permetta di valutare correttamente a quale soggetto rivolgersi.

4.2.1 Criteri di selezione

La scelta del partner costituisce, come accennato, un adempimento di pregnante importanza che impone di seguire precisi criteri di selezione.

I criteri di selezione da valutare imprescindibilmente per individuare con maggiore oculatezza possibile il partner sono:

1. la capacità di fornire una prestazione altamente qualificata;
2. l'esperienza del fornitore nella conservazione digitale in generale e, in particolare, per la specifica tipologia di documenti da conservare, (come nel caso di documenti fiscali o sanitari);
3. la conoscenza ed il rispetto della normativa privacy, anche in considerazione di quanto già esposto nei precedenti paragrafi e della nuova formulazione dell'art. 44 del Codice dell'amministrazione digitale¹⁶. Con particolare riferimento alla conservazione digitale dei documenti sanitari, è indispensabile che il responsabile conosca e applichi perfettamente le misure di sicurezza per il trattamento dei dati sanitari, quali:

¹⁶ Il nuovo art. 44 del CAD prescrive che il responsabile che gestisce il sistema di conservazione deve necessariamente operare d'intesa “con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza”.

- l'adozione di idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e del trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati, sottoscrizione del documento informatico, etc.);
- il permettere il trattamento dei dati personali, anche di natura sensibile, solo a responsabili o incaricati dotati di credenziali di autenticazione che abbiano superato una procedura di autenticazione (strong authentication) relativa a uno specifico trattamento o a un insieme di trattamenti (ciò consente di fornire le garanzie rispetto all'accesso da parte dei vari operatori specificatamente autorizzati);
- l'adozione di una procedura per la gestione delle credenziali di autenticazione, che consistono in un codice per l'identificazione del responsabile o dell'incaricato associato a una parola chiave riservata (di almeno 8 caratteri alfanumerici) conosciuta solamente dal medesimo. Le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere automaticamente disattivate dal sistema, anche nel caso di perdita della qualità che consentiva al responsabile o all'incaricato l'accesso ai dati personali;
- l'assegnazione o associazione individuale ad ogni responsabile o incaricato di una o più credenziali per l'autenticazione (che non può e, quindi, non deve essere assegnato ad altri incaricati, neppure in tempi diversi) per l'accesso al programma informatico (con creazione di profili differenziati per l'accesso agli archivi e procedure di autenticazione distinte per i vari profili individuati);
- l'adozione di un idoneo sistema di back up e restore dei dati che garantisca il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni;

- l’effettuazione di un trattamento disgiunto dei dati idonei a rivelare lo stato di salute contenuti nelle banche dati dagli altri dati personali che permettono di identificare direttamente gli interessati (separazione logica dei dati idonei a rivelare lo stato di salute dagli altri dati personali trattati per scopi amministrativo-contabili);
 - l’utilizzazione di software composti da una struttura modulare delle varie cartelle elettroniche in modo da garantire la separazione fra le diverse categorie di dati rispetto alle finalità del trattamento e ai soggetti che vi accedono¹⁷;
 - l’individuazione di procedure tecnico-organizzative idonee a ridurre al minimo, nel processo di dematerializzazione dei referti, l’incidenza di operazioni manuali, in quanto caratterizzate da un elevato tasso di errore¹⁸.
4. l’ampiezza dei servizi offerti, tra cui, nel caso di conservazione di documenti sanitari, la possibilità di sviluppare strumenti di audit ex post degli accessi agli archivi contenenti i referti, sia nella fase di memorizzazione PACS, sia in quella di archiviazione storica, definendo un processo di management dei log che sia in grado di rappresentare con completezza - per una determinata profondità temporale opportunamente commisurata alle esigenze di controllo sul corretto utilizzo della base di dati e degli accessi da parte del titolare del trattamento - l’insieme delle operazioni effettuate sui referti, nonché di garantire l’inalterabilità dei log memorizzati¹⁹;

¹⁷ Tali prescrizioni sono delle Misure di sicurezza per il trattamento dei dati sanitari in conformità e rispondenza al D. Lgs. n. 196 del 30/6/2006, contenute nel Codice Privacy e nel relativo Allegato B (Disciplinare tecnico in materia di misure di sicurezza), oltre che negli specifici provvedimenti del Garante in materia.

¹⁸ Così come prescrivono le Linee guida in tema di referti on-line, contenute nel Provvedimento del Garante Privacy del 19 novembre 2009.

¹⁹ Così come prescritto dal Provvedimento del Garante per la protezione dei dati personali del 26 novembre 2009.

5. le garanzie tecnologiche e di sistema offerte dal fornitore in relazione agli standard di sicurezza informatica, per esempio, in riferimento alla protezione dei dati personali e delle informazioni scambiate. Per quanto concerne la sicurezza informatica della globalità del sistema di conservazione, le norme ISO/IEC 27001 e 27002 e la specifica ETSI TS 102 573 (“Policy requirements for trust service providers signing and/or storing data for digital accounting”) dettano le condizioni per la gestione e valutazione di sistemi sicuri ed affidabili per la conservazione elettronica delle informazioni;
6. il possesso di eventuali certificazioni sui servizi proposti;
7. il prezzo del servizio;
8. le referenze;
9. il livello di professionalità del personale;
10. le dimensioni ed il grado di umidità dei locali in cui saranno conservati gli eventuali documenti analogici non distrutti in seguito al processo di conservazione, verificando preventivamente che siano stati rispettati gli standard richiesti dalla normativa europea;
11. l’eventuale accreditamento del fornitore ex art. 44-bis del CAD. 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. I certificatori e i conservatori che intendono conseguire tale riconoscimento devono, quindi, presentare domanda di accreditamento presso DigitPA secondo le regole, ove compatibili, previste dall’art. 26, 27, 29 e 31 del CAD²⁰. La domanda di accreditamento si conside-

²⁰ Il richiedente, se soggetto privato, dovrà quantomeno:

rerà accolta qualora non verrà comunicato all’interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa. A seguito dell’accoglimento della domanda, il DigitPA disporrà l’iscrizione del richiedente in un apposito elenco pubblico, tenuto dal DigitPA stesso e consultabile anche in via telematica, ai fini dell’applicazione della disciplina in questione; da questo momento in poi il conservatore/certificatore accreditato potrà qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni;

12. l’adozione di moduli organizzativi adeguati ai sensi del D. Lgs. n. 231 dell’8.6.2001 rubricato “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell’articolo 11 della legge 29 settembre 2000, n. 300.)”.

4.2.2 Il contratto di outsourcing: caratteristiche generali

La delega verso l’esterno avviene, in genere, mediante la sottoscrizione di un contratto di *outsourcing*, quindi, attraverso un

a) avere forma giuridica di società di capitali e un capitale sociale non inferiore a 200.000 Euro (tale requisito non è richiesto per le PA).

b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell’articolo 26 del decreto legislativo 1° settembre 1993, n. 385.

La domanda di accreditamento dovrà, inoltre, contenere:

a) il profilo professionale del personale responsabile della conservazione o della certificazione e l’impegno al rispetto delle regole tecniche;

b) attestazione dell’affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione e conservazione;

c) dichiarazione di utilizzo di personale dotato delle conoscenze specifiche, dell’esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia dei processi di conservazione e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all’articolo 71;

d) attestazione dell’applicazione di procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;

e) attestazione dell’affidabilità e della sicurezza dei sistemi utilizzati.

rapporto contrattuale strutturato, di medio-lungo termine, rivolto all’acquisizione di servizi (in tal caso la conservazione sostitutiva) presso un terzo “fornitore”. Con la stipulazione di questa tipologia di contratto, il terzo fornitore non assume il ruolo di un mero professionista, chiamato ad adempiere esclusivamente alle mansioni assegnategli: tra il terzo e l’ente cliente si viene a creare, infatti, uno stretto rapporto di collaborazione, una vera e propria *partnership*. E, infatti, l’*outsourcer* non si limita ad effettuare la sola conservazione dei documenti informatici: il suo intervento comprende, in genere, anche lo studio dei flussi documentali digitalizzati, la riparazione di eventuali guasti al sistema, la ricerca di modifiche da apportare al servizio a seguito di evoluzioni tecnologiche o normative, la fornitura di potenziali applicazioni connesse al servizio di conservazione (per es. il backup remoto dei dati) o anche la somministrazione di sistemi di messaggistica istantanea, etc.²¹ L’*outsourcer*, pertanto, sarà sempre più spesso chiamato a seguire anche il cammino dell’ente/ cliente, le sue evoluzioni e i suoi cambiamenti organizzativi e dovrà garantire che il passaggio eventuale del compito di responsabile della conservazione ad altro soggetto avvenga celermente e senza traumi per il cliente.

A tal proposito, sarà sempre utile richiedere al proprio *outsourcer* l’utilizzo di tecnologie e sistemi compatibili e interoperabili. In ordine a tale profilo, è utile segnalare l’esistenza di uno standard a cui fare riferimento per i file di chiusura dei lotti appartenenti all’archivio di conservazione: si tratta di uno standard UNI/SInCRO, ovvero la Norma UNI 11386:2010 – Supporto all’Interoperabilità nella Conservazione e nel recupero degli Oggetti digitali (SInCRO), che è stata pubblicata lo scorso anno.

²¹ Si parla dell’evoluzione dell’outsourcing in SaS (Software as a Service), un contratto con cui l’azienda sceglie di esternalizzare tutto ciò che non riguarda specificamente il suo core business, ma che comunque resta di supporto all’organizzazione aziendale e può essere curato mediante software applicativi gestiti e forniti da terzi (per es. business intelligence, gestione delle relazioni con i clienti, webmail, data integration, ecc.).

4.2.3 Cosa deve prevedere un buon contratto di outsourcing

Il contratto di outsourcing è un contratto *atipico* che la maggior parte della dottrina ha inteso inquadrare nell’ambito dell’appalto di servizi e della somministrazione. In genere, al pari di quest’ultima, il servizio fornito mediante la stipulazione di un contratto di *outsourcing* ha un decorso pluriennale; da ciò la necessità di prevedere, sin dalle fasi di preparazione, particolari meccanismi di composizione delle controversie che permettano di salvare il contratto mediante forme di rinegoziazione o transazione.

- Gli allegati al contratto di outsourcing: gli SLA
Trattandosi di accordi particolarmente complessi, soprattutto per quanto concerne gli standard applicativi, a queste tipologie contrattuali vengono, in genere, aggiunti degli allegati che prendono il nome di *Service Level Agreements* (SLA) - Contratti di qualità e servizio.

Negli SLA vengono ripresi più in dettaglio, e trattati dal punto di vista tecnico, il servizio fornito e le obbligazioni reciproche delle parti, già contenute nell’accordo principale. Vengono, inoltre, definiti puntualmente i livelli qualitativi che l’*outsourcer* dovrà mantenere, i criteri di misurazione degli stessi, le procedure di monitoraggio ed eventuali obblighi aggiuntivi che si rendano indispensabili in relazione alla riservatezza dei dati e alla sicurezza delle informazioni scambiate.

Con riferimento alla conservazione della documentazione sanitaria, ad esempio, sarà utile obbligare il proprio *outsourcer* all’utilizzo di standard documentali che permettano di garantire nel tempo l’interoperabilità²².

²² In tema di conservazione di lungo periodo, come quella prevista per la documentazione sanitaria, è di particolare importanza il rispetto delle regole individuate dalla norma UNI (UNI 11386:2010 SInCRO) relative alla creazione dell’indice di conservazione, così da garantire nel tempo l’interoperabilità fra i sistemi di conservazione.

Nella fase che precede la stipulazione, è necessario chiarire correttamente l’oggetto del contratto, specificando quali incarichi restano nell’area di competenza di ciascuna parte ed evidenziando i rispettivi obblighi e diritti.

Sarà opportuno prevedere e progettare eventuali piani di *disaster recovery*, ovvero procedure di emergenza e soccorso, imprescindibili qualora eventi anomali e inaspettati producano la temporanea interruzione del servizio.

È in questa fase, inoltre, che sarà necessario definire i c.d. accordi di segretezza. Data la delicatezza delle informazioni e dei dati oggetto del servizio di conservazione sostitutiva, soprattutto nel caso di conservazione di dati sanitari, è infatti opportuno inserire questa tipologia di obbligazioni tra le parti, affinché si mantenga un rigoroso riserbo sul contenuto dei documenti scambiati.

- Contenuto minimo del contratto di outsourcing

Passando al contratto vero e proprio, esso dovrà delineare in linea generale:

- le modalità di implementazione del servizio;
- la durata prevista per la fase di *start up*, la cui descrizione tecnica sarà accuratamente delineata nello SLA;
- l’iter da seguire nel processo di conservazione sostitutiva;
- lo sviluppo di una reportistica on line che faciliti il monitoraggio del servizio offerto;
- le modalità di conservazione dei documenti e le misure di sicurezza adottate ai sensi del Codice dell’amministrazione digitale;
- le regole di ingresso nell’archivio, prevedendo un accesso riservato ai soli utenti che si identificano (ad esempio, mediante specifici ID e Password), anche quando non siano presenti dati personali; mentre, nel caso questi siano presenti (ad esempio nei documenti contenenti dati sanitari),

- il contratto dovrà prevedere diversi profili di autorizzazione per l'accesso agli archivi e procedure di autenticazione distinte per i vari profili individuali;
- le responsabilità dell'*outsourcer* e le speciali polizze assicurative per particolari tipologie di danni e/o eventi e delle penali;
 - clausole specifiche sulla tutela della proprietà industriale. Poiché durante l'esecuzione del contratto l'*outsourcer* potrebbe imbattersi in documenti che riguardino il *know how* del suo cliente, si rende opportuno specificare l'assoluta riservatezza delle informazioni, di esclusiva proprietà dell'impresa cliente. Di conseguenza, l'*outsourcer*, per tutta la durata del contratto, dovrà impegnarsi a non utilizzare tali informazioni, se non per i fini previsti, obbligandosi a cessarne l'uso al termine del rapporto contrattuale. Ovviamente, questo varrà anche per l'impresa cliente nei confronti del *know how* del suo fornitore;
 - clausole utili a chiarire i tempi di fornitura del servizio, scandendo le varie fasi del procedimento di conservazione;
 - la programmazione per le manutenzioni che si renderanno opportune, prevedendo la necessità di averne notizia con congruo anticipo;
 - i controlli che potranno essere legittimamente effettuati dall'impresa/ente cliente per verificare il rispetto degli standard di qualità nella fornitura del servizio, specificando le modalità mediante le quali potrebbe avvenire tale accertamento e prevedendo, ad esempio, l'accesso pacifico nei luoghi fisici di conservazione dei documenti;
 - le modalità di calcolo del corrispettivo per l'erogazione del servizio (in genere calcolato su base mensile o, più spesso, conteggiato sul numero di documenti portati in conservazione) ed eventuali rinegoziazioni delle tariffe

che si rendessero opportune al verificarsi di eventi ben delineati;

- l'obbligo per le parti, qualora si verificasse lo scioglimento del contratto, di restituire o distruggere qualsiasi dato, documento o informazione ed un impegno dell'*outsourcer* a che il passaggio del servizio di conservazione sostitutiva ad eventuale altro fornitore avvenga nella maniera più semplice.
- Contenuti extra del contratto di outsourcing

Nel caso in cui ad essere esternalizzato sia il processo di conservazione digitale dei documenti sanitari, sarebbe opportuno che il relativo contratto di outsourcing prevedesse altresì:

- l'utilizzazione di una conservazione crittografata o, in alternativa, l'impiego di forme di anonimizzazione dei dati identificativi;
 - la tracciabilità degli accessi e delle operazioni effettuate (accountability);
 - protocolli di comunicazione sicuri con standard crittografici per la comunicazione elettronica tra diversi titolari in un FSE (Fascicolo Sanitario Elettronico);
- Per quanto attiene, più in particolare, i referti on line, il contratto è auspicabile contenga:
1. protocolli di comunicazione sicuri, basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati, con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (protocolli https ssl – Secure Socket Layer);
 2. tecniche idonee ad evitare la possibile acquisizione delle informazioni contenute nel file elettronico nel caso di sua memorizzazione intermedia in sistemi di caching, locali o centralizzati, a seguito della sua consultazione on-line;

3. utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di strong authentication;
4. disponibilità limitata nel tempo del referto on-line (massimo 45 gg.);
5. possibilità, da parte dell'utente, di sottrarre alla visibilità in modalità on-line o di cancellare dal sistema di consultazione, in modo complessivo o selettivo, i referti che lo riguardano;
6. idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad esempio, in relazione alla possibilità di consultazione, modifica e integrazione dei dati), prevedendo il ricorso alla *strong authentication*, con utilizzo di caratteristiche biometriche nel caso del trattamento di dati idonei a rivelare l'identità genetica di un individuo;
7. separazione fisica o logica dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali trattati per scopi amministrativo-contabili;
8. procedure che rendano immediatamente non disponibili per la consultazione on-line o interrompano la procedura di spedizione per posta elettronica dei referti relativi a un interessato che abbia comunicato il furto o lo smarrimento delle proprie credenziali di autenticazione all'accesso al sistema di consultazione on-line o altre condizioni di possibile rischio per la riservatezza dei suoi dati²³.

²³ Linee Guida in tema di referti on line, adottate con Provvedimento del Garante per la protezione dei dati personali del 19 novembre 2009.