

# L'archivio nell'era della sua riproducibilità tecnica

09/2006, A.Cammozzo

*Le recenti tendenze tecnologiche, ben rappresentate dal codice per la Pubblica Amministrazione digitale, impongono un "supporto" digitale alla futura generazione di documenti amministrativi. La duplicabilità e la agevole alterabilità dei documenti digitali costituisce un grande beneficio in molti campi, ma rappresenta un ben documentato problema nel caso di archivi che nell'immutabilità dei contenuti hanno la loro ragion d'essere. Il matrimonio tra archivi e informatica sembra quindi essere tra quelli più litigiosi, ma proprio i rispettivi "difetti" possono forse essere la chiave della sua tenuta.*

## Il naufragio del supporto

L'industria dell'intrattenimento definisce i propri prodotti "contenuti". Da quando musica, film, immagini e testi possono essere rappresentati digitalmente hanno perso il nome e il volto dei supporti sui quali erano *memorizzati*: disco, videocassetta, dvd, libro. Il naufragio del supporto si è coerentemente accompagnato con la cosiddetta pirateria, ovvero la prassi della replicazione indiscriminata del contenuto, agevolato dalla diffusione e capacità delle reti di telecomunicazioni. L'industria dei media, dopo aver entusiasticamente abbracciato il digitale, da anni cerca di impedire la replicabilità dei contenuti attraverso discusse misure, inefficaci al punto da richiedere il supporto di leggi tanto severe quanto controverse e impopolari.

Questa esperienza appare analoga a quanto avviene con il protratto sforzo di digitalizzare l'archiviazione dei documenti: da una parte l'esigenza archivistica di autenticità e immutabilità del documento, dall'altra l'intrinseca mutevolezza di un *file* elettronico. I vantaggi connessi con la flessibilità del calcolatore e il potenziamento dei mezzi a corredo, contro l'intrinseca volatilità di un documento che si vorrebbe perenne. Il supporto cartaceo rivela di essere più di un semplice vettore di informazione e abbandonarlo fa venir meno le garanzie di *genuinità di forma e materia* che esso porta con se, per il fatto di essere esso stesso la *forma* e la *materia*.

Il contenuto digitale, unito alla telematica, offre tuttavia una sua forma peculiare di persistenza proprio attraverso la replicazione: i *file*, se replicati in luoghi diversi della rete, più difficilmente andranno persi per via di guasti, cancellazioni volontarie o accidentali. Se una copia del *file* venisse manomessa, risulterebbe facile rilevare l'alterazione attraverso il confronto con le altre copie. Il rischio connesso a questa forma di persistenza è l'*oblio*: se tutti i diversi custodi, indipendentemente, perdono interesse nel detenere il *file* e lo cancellano, questo sparirà definitivamente.

## Come rendere persistente e *autentico* il digitale

Il problema dell'alterabilità dei documenti digitali è ben noto e dibattuto, e si è tentato di porvi rimedio con mezzi più o meno tecnologici. La prima forma di alterazione da combattere è la *manomissione* di un documento archiviato, specie in una forma che alteri la volontà di chi lo sottoscrive. La seconda alterazione è quella dovuta al *degradarsi* del supporto (solitamente magnetico o ottico) sul quale il documento è conservato, dovuto al tempo o a danni. La terza forma di alterazione è quella, subdola, di un documento che contiene in se stesso *elementi attivi*, istruzioni, e che pur rimanendo inalterato nella sua forma di rappresentazione binaria, muta l'aspetto con cui si presenta. Come vengono affrontate queste alterazioni?

1. Crittografia e firma digitale.

L'applicazione di procedure di cifratura matematica attraverso algoritmi codificati per calcolatore sembra l'unico modo per garantire un documento dalla sua manomissione: l'associazione della particolare chiave con la quale uno specifico documento viene cifrato a un *certificato* legato all'identità di una determinata persona diventa l'analogo della *firma*. Per una serie di esigenze funzionali la firma è soggetta a scadenza e a revoca: una singola persona potrebbe avere più firme sia in momenti di tempo successivi, ma anche contemporaneamente. Un documento potrebbe risultare quindi tecnicamente firmato in modo corretto, ma con una firma priva di validità a partire di un dato momento, il che renderebbe critica la sua datazione e la verifica della validità della firma una volta che questa sia scaduta.

## 2. Custodia ininterrotta.

Benché siano in grado di contenere un volume di dati molto elevato in confronto ai supporti caracei, i supporti per *file* digitali hanno una durata misurabile in alcune decine di anni. Questo li rende inadatti a conservazione di documenti destinati alla conservazione, a meno di prevedere periodicamente il loro riversamento sostitutivo su supporti freschi, possibilmente più capaci ed aggiornati, al passo con le innovazioni tecnologiche. Anche supponendo che gli archivi vengano conservati esclusivamente su supporti non riscrivibili (cioè non manomettibili) sussiste il pericolo che vi possano essere state delle alterazioni nel corso dei riversamenti, privando in sostanza il supporto di qualsiasi autorevolezza.

Per supplire a questa carenza non resta che affidarsi alla affidabilità di chi lo ha conservato, e investire di fiducia l'ininterrotta catena di custodia dei supporti sui quali il dato documento è stato conservato.

## 3. L'anello mancante: i formati aperti, i programmi leali.

Per non vanificare lo sforzo tecnologico che la firma digitale costituisce, occorre scongiurare la possibilità che un documento appaia in un modo alla firma e in modo diverso in un momento successivo, pur rimanendo inalterata la sua rappresentazione digitale, la sua impronta e di conseguenza la validità della firma. Questo comportamento ingannevole è possibile ricorrendo all'uso di formati, quali quelli solitamente usati da elaboratori di testi, che consentono l'inclusione, oltre al testo del documento, di istruzioni per il programma stesso (ad es. le cd. *macroistruzioni*). Occorre quindi che la firma vada applicata *solo* a documenti che garantiscano la loro lealtà al firmatario attraverso la loro completa trasparenza, ovvero che questi documenti siano rappresentati *esclusivamente* in un formato completamente aperto e documentato. Una volta assicurata la lealtà del formato dati, va garantita quella del programma che deve leggere e rappresentare il documento: con assoluta certezza esso non deve contenere istruzioni che possano alterare selettivamente la rappresentazione fedele del documento.

## Aspetti problematici

In occasione di un blocco completo di un importante aeroporto nazionale, un responsabile ha giustificato il gravissimo evento come un "normale guasto software". Affermazione che richiama la frase: *la tecnologia si chiama tale fintanto che non funziona, poi si chiama tecnica*. Le tecniche archivistiche hanno certamente avuto un tempo in cui, in attesa di affinamenti, si sono dimostrate inaffidabili, imperfette, inefficienti, ma per almeno un secolo hanno dimostrato di essere almeno solo perfezionabili. L'informatica, specie nel software, sta affrancandosi difficilmente dal marchio dell'inaffidabilità, e con costi economici e tecnologici molto alti.

In merito a quanto sopra evidenziato possono evidenziarsi queste criticità:

### 1. Crittografia: una cassaforte ad apertura temporizzata.

Tutte le tecniche di cifratura sono soggette a attacchi di tipo o matematico, che ne minano le radici svelando la chiave di cifratura senza sforzo, o di tipo *forza bruta* ovvero per ripetuti

tentativi ad esaurimento fino all'individuazione della chiave di cifratura. Il primo tipo di attacco dipende dall'ingegno dei matematici, che ha dimostrato di evolvere e affinarsi almeno quanto la tecnologia, dalla quale invece dipende la facilità del secondo tipo di attacco.

La robustezza di una chiave crittografica, insomma, dipende dal tempo. Non vi è nessuna garanzia, e anzi sembra verosimile vi sia quella opposta, che in un futuro non troppo remoto quella che consideriamo cifratura robusta divenga poco più di una banale sostituzione monoalfabetica, usata per millenni, ma oggi attaccabile agevolmente da qualsiasi personal computer.

Come garantire quindi l'autenticità storica dei documenti custoditi negli archivi, se qualsiasi soggetto dotato di sufficienti mezzi e interesse potrà generare documenti autentici con firme, supporto, forma indistinguibili da quello originale? Sembra che l'unico mezzo sia quello della custodia ininterrotta, a garanzia della non manomissione di un documento comunque manomettibile in modo da non lasciare traccia alcuna. Ma allora a che serve la firma digitale?

## 2. La custodia ininterrotta: una fatica di Sisifo.

Come già detto, data la intrinseca deperibilità dei mezzi informatici non riscrivibili, questi vanno continuamente rigenerati riversandoli in nuovi supporti affidabili. Anche confidando nella futura tecnologia che ci offrirà supporti sempre più affidabili e capaci, ci aspetta il compito di spingere su per la china del tempo il nostro patrimonio documentale, nella consapevolezza che questo nel tempo si accresce e si degrada, avendo cura di non lasciare nulla indietro: non ci saranno feriti. Sappiamo già ora che questo non sarà possibile. Se possiamo sperare di recuperare la forma e la funzionalità di un archivio cartaceo riscoperto dopo un secolo e più, questo è impensabile per quello digitale non adeguatamente custodito e rigenerato. Supporti più fragili della carta, quali le pellicole chimiche (foto e video) ci hanno dimostrato che questa perdita è possibile, ma a differenza dei supporti analogici, il cui degrado è progressivo e la cui immagine svanisce col tempo, quelli digitali, specie se compressi, vengono irrimediabilmente smarriti nella loro interezza.

## 3. La firma digitale: un ossimoro?

Le numerose problematiche di sicurezza, oltre a quelle già citate insite nella cifratura, rendono la firma digitale un elemento problematico. Tra tutte: l'obbligo di conservare i certificati per soli dieci anni in capo degli enti certificatori, la debolezza di una catena estremamente complessa (e costosa) di fiducia che in ultimo si esaurisce in un PIN di pochi numeri o peggio in una impronta digitale che facilmente potrà essere rilevata dal supporto stesso che contiene la firma (la smart-card); la fiducia in un sistema tecnologico centrato su personal computer che sono storicamente i sistemi informatici più deboli sul piano della sicurezza. Questi elementi di insicurezza non sarebbero così problematici se la firma digitale non fosse ammantata, come ogni complessa macchina tecnologica, di scientifica sicurezza. Dovrebbe essere invece chiaro che la firma digitale non è più affidabile di quella applicata a mano con inchiostro indelebile su un foglio di carta, e che quindi anche a quella vanno applicate le cautele usate per questa.

## 4. Formati aperti, programmi leali: una strada praticabile.

Benché lo standard di mercato rimanga orientato nella direzione opposta, sta maturando nelle pubbliche amministrazioni la consapevolezza che per una serie di motivi, non solo archivistici, vanno adottati esclusivamente formati aperti: per il ruolo cardine svolto nei confronti del cittadino, per evitare la dipendenza da fornitori specifici e dalle sue scelte tecnologiche (*data lock-in*), per garantire la persistenza dell'accesso ai propri documenti. La scelta di formati aperti consentirà la possibilità di escludere in modo certo che vi siano elementi dinamici nel documento che possano alterarne l'aspetto.

Diverso il problema dei programmi sicuri e leali, ossia di programmi che in modo certo facciano

solo quello che ci si attende che facciano. Che non assumano cioè comportamenti che possano alterare l'aspetto del documento sia alla firma che dopo in modo accidentale (per effetto di errori di programmazione) o deliberato (per intenzione del programmatore o per intervento di altri programmi come virus). Un inizio di soluzione può essere dato dai programmi a codice sorgente aperto (*free software* o *open source*) la cui ispezionabilità fornisce elementi di maggior garanzia rispetto a programmi proprietari. Tuttavia la costruzione di un sistema informatico complesso a prova di errori e completamente affidabile è ancora un obiettivo assai ambizioso.

## Cosa manca

Dai "difetti" della tecnica archivistica e della tecnologia informatica possono nascere delle proposte per conciliare gli inevitabili contrasti che l'unione informatica/archivistica sembra suscitare.

L'informatica non ha mai cercato, perché mai lo ha ritenuto utile, studiare di operare con un supporto immutabile, ingegnerizzato per resistere al tempo, interoperabile, immediato, quale è la carta con l'inchiostro. L'archivistica non ha, forse perché troppo oneroso, confidato nella replicazione massiccia dei documenti per garantire la loro conservazione e massima accessibilità, con l'eccezione di pochi *documenti vitali* (ad es. gli statuti della città, come nel caso di Padova).

La proposta quindi potrebbe articolarsi in due direzioni, ortogonali e quindi complementari:

### 1. Archivio a *persistenza statistica* attraverso replicazione massiccia.

Gli archivi informatici digitali (in particolare quelli storici) andrebbero replicati in diverse sedi, su diversi supporti, in diverse mani, e periodicamente confrontati, alla ricerca di danneggiamenti o manomissioni. Ogni alterazione diverrebbe facile da rilevare, garantendo al *documento distribuito* una garanzia statistica da manomissione e deperimento. Piuttosto che confidare in supporti inalterabili e costosi, la persistenza andrebbe garantita attraverso la replicazione simultanea in più copie su supporti ordinari e il continuo confronto della coerenza dei dati.

Rimarrebbe beninteso l'obbligo della rigenerazione, ma una rete archivistica ben organizzata potrebbe garantire la persistenza dei dati con il confronto periodico dei contenuti dei rispettivi archivi, rigenerando i solo nel caso del loro effettivo danneggiamento.

### 2. Studio di un supporto digitale persistente.

Nella direzione opposta alla precedente, andrebbe richiesto all'industria delle memorie di massa uno sforzo nell'individuazione di supporti dotati delle caratteristiche di immutabilità della carta, se non migliori, unite alla compattezza del supporto digitale. Un supporto di questo genere non sarebbe di leggibilità immediata, richiedendo comunque la mediazione di un calcolatore, ma potrebbe durare secoli.

Questa seconda strada si presenta come più costosa e incerta della prima, richiedendo uno sforzo tecnologico che va in una direzione opposta a quello attualmente in atto. Tuttavia nelle pieghe della ricerca si nascondono tecnologie senza apparente possibile impiego (come l'adesivo troppo debole dei post-it), e potrebbe bastare una forte richiesta da parte della comunità archivistica per rendere l'impegno evidente ed utile.

## Riferimenti:

G. Bonfiglio-Dosio, *Primi passi nel mondo degli archivi*, CLEUP, Padova, 2005

S. Pigliapoco, *La memoria digitale delle amministrazioni pubbliche*, Maggioli, 2005