LA SICUREZZA NELLA CONSERVAZIONE DIGITALE

A. SIMONETTA*, F. RUGGIERI**

SOMMARIO

1. La definizione del problema

Nell'epoca in cui le informazioni sono rappresentate in misura sempre maggiore in formato digitale la loro conservazione assume un ruolo chiave e, allo stesso tempo, si rende necessario affrontare problematiche relative alla sicurezza, al reperimento e al mantenimento a lungo termine delle informazioni stesse.
Non a caso la disponibilità di informazioni pressoché intatte provenienti da culture antiche risalenti ai primi secoli D.C. o addirittura a periodi storici antecedenti è stata possibile non soltanto con l'utilizzo di supporti analogici persistenti ma, soprattutto, grazie all'opera di centri di conservazione e migrazione dei dati da un formato all'altro.
Sebbene la tecnologia abbia fatto passi da gigante nell'ambito dell'archiviazione digitale, sia per densità di memorizzazione sia per velocità di accesso, lo stesso non si può affermare rispetto alla conservazione integra dei dati nel tempo. Infatti, tutti i supporti di memorizzazione presentano criticità di persistenza che dipendono fortemente da aspetti fisici del supporto stesso.
Studi recenti[1] stanno valutando la possibilità di memorizzare informazioni attraverso l'utilizzo della nanomeccanica. Analogamente alla tecnica utilizzata nelle vecchie schede perforate, si utilizzano fori nanoscopici per codificare bit attraverso un processo di incisione termica (reversibile) su sottili fogli di polimeri.

* Consulenza per l'Innovazione Tecnologica - Direzione Generale INAIL.
** FIR DIG Consultants di RUGGIERI F & C sas.

1 B. GOTSMANN, A.W. KNOLL, R. PRATT, J. FROMMER, J.L. HEDRICK, AND U., *Duering, Designing Polimers to Enable Nanoscale Thermomechanical Data Storage*, Advanced Functional Materials. 2010, 20, *1276-1284*.

Questo sistema permette di archiviare in un centimetro quadrato fino ad un TeraBit e, grazie alle caratteristiche fisiche del supporto, di preservare le informazioni (a una temperatura non superiore a 85ºC) per circa un decennio. Proprietà del tutto confrontabili alle classiche memorie flash.
La conservazione e il reperimento delle informazioni digitali spesso si misura anche con difficoltà tecnologiche quali: sistema di codifica proprietari non più in commercio, software e hardware obsoleti, utilizzo di protocolli di comunicazione non più supportati.
Infatti, se si dovessero recuperare dei dati presenti su di un semplice floppy disk (estinto nell'ultimo decennio) potremmo avere qualche difficoltà, sempre che il supporto stesso non sia smagnetizzato.
Il sistema di conservazione va poi gestito con dovute misure - preferibilmente sulla base di indicazioni fornite da norme - atte ad assicurare una adeguata sicurezza informatica.
Allo stato attuale, in mancanza di norme specifiche che disciplinano gli aspetti legati alla sicurezza, la gestione della conservazione documentale è trattata come un "normale" servizio le cui caratteristiche e modalità di erogazione sono descritte in un contratto. Questo contratto viene troppo spesso stipulato tra parti aventi ben diversa competenza tecnica e quindi in situazioni in cui il cliente si può trovare in condizioni di inferiorità conoscitiva rispetto al fornitore[2].

2. Il quadro normativo

Il quadro normativo italiano nell'ambito della conservazione dei documenti e delle problematiche ad essa connesse è piuttosto articolato sia per la complessità della materia trattata, sia per la continua evoluzione tecnologica che non ha permesso di fissare in maniera definitiva un quadro di riferimento consolidato. Il presente articolo si basa sulle norme tecniche e giuridiche in vigore al 31 gennaio 2011.
Tra i primi dispositivi giuridici relativi alla conservazione documentale, la legge finanziaria del 1994 (n. 537 del 24 dicembre 1993) nell'art. 2 relativo alle semplificazione e accelerazione dei procedimenti amministrativi, stabiliva la possibilità di conservare i documenti su supporto ottico (in alternativa ad altri strumenti) purché le procedure utilizzate fossero conformi alle allora emanande regole tecniche dell'Autorità per l'informatica nella Pubblica Amministrazione (Deliberazione AIPA n. 15 del 28 luglio 1994 sostituita integralmente dalla Deliberazione 24 del 30 luglio 1998 - Regole tecniche per l'uso di supporti ottici).
La citata Deliberazione 24/1998 enunciava in modo molto particolareggiato le modalità per l'archiviazione ottica dei documenti.

2 Si veda a questo riguardo l'ormai consolidato *The Market for Lemons: Quality Uncertainty and the Market Mechanism*, di GEORGE AKERLOF, *The Quarterly Journal of Economics*, Vol. 84, No. 3 (Aug. 1970), *pp. 488-500*.

In seguito l'allora AIPA, poi Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA), decise di sostituire integralmente la Deliberazione n. 24/98 con la Deliberazione n. 42/2001 con lo scopo di migliorare le regole tecniche relative alla conservazione dei dati e ampliare la tipologia di supporti di memorizzazione a quelli non ottici. Poiché tali regole prevedevano l'applicazione della firma digitale all'insieme dei documenti conservati, l'esibizione del singolo documento estratto dall'insieme presentava alcune difficoltà. Inoltre le definizioni di "*documento informatico*" e di "*firma digitale*" non erano coerenti con quelle presenti nel Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (decreto del Presidente della Repubblica n. 445/2000).
Per tali ragioni il CNIPA, confrontandosi con gli operatori del settore ed esperti accademici, emanava la Deliberazione n. 11/2004 ancora oggi in vigore.
L'esigenza crescente di gestire documenti in formato elettronico è correlata alle linee di indirizzo che nel tempo hanno indicato la strada della dematerializzazione come l'unica possibile per un risparmio economico ed ambientale della PA. Infatti uno degli obiettivi del piano strategico per la PA (Piano e-Gov 2012) è la digitalizzazione.
La svolta per la "scomparsa della carta" nella PA avviene con l'entrata in vigore del Codice dell'amministrazione digitale (Decreto legislativo n. 82 del 7 marzo 2005) il primo gennaio 2006.
Il Codice dell'amministrazione digitale è il pilastro su cui poggia il progetto di digitalizzazione della PA definito nel Piano industriale del 2008.
Anch'esso è stato oggetto di adeguamenti da parte del legislatore: decreto legislativo n. 159 del 4 aprile 2006 e Decreto Legge "anticrisi" 185/2008 convertito in Legge n. 2/2009 e, da ultimo, decreto legislativo n. 235 del 30 dicembre 2010.
Con riferimento ai documenti informatici e alla loro conservazione, alcune modifiche ed integrazioni introdotte da questo ultimo provvedimento (artt. 1 e 15) meritano un approfondimento.
All'art. 1, comma 1, del D.Lgs. n. 82/05 sono aggiunte le definizioni relative a tre tipologie di "copia":

a) "copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto" (lettera i-*bis*);
b) "copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto" (lettera i-*ter);*
c) "*copia informatica di documento informatico:* il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari" (lettera *i-quater).*

Si noti la differenza tra la copia informatica (lettera i-*bis*) e quella per immagine su supporto informatico (lettera i-*ter*): la prima tratta il caso in cui solo la semantica di un documento analogico è riportata in un documento informatico, mentre la seconda è la classica digitalizzazione dell'immagine del documento analogico. L'ultima tipologia di copia (lettera i-*quater*), infine, riguarda quello che comunemente viene chiamato "cambio di formato", ad esempio da ".doc" a ".docx" o a ".pdf".
Un altro elemento di interesse riguarda la modifica all'art. 22 del D.Lgs. n. 82/2005 con la quale si attribuisce alla copia elettronica di un documento analogico l'idoneità "*ad assolvere gli obblighi di conservazione previsti dalla legge*" (art. 22, comma 4). In particolare situazioni queste modifiche riguardano i seguenti commi:

1) "documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, **spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali**" (art. 22, comma 1);
2) "copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico, **se la loro conformità è attestata da un notaio o da altro pubblico ufficiale** a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71" (art. 22, comma 2);
3) "copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico **nel rispetto delle regole tecniche di cui all'articolo 71**" (art. 22, comma 3).

Sempre con le modifiche introdotte dal D. Lgs 235/2010, già anticipate con la legge n. 2/2009, si lascia la possibilità di individuare - con decreto del Presidente del Consiglio dei Ministri - classi di documenti per i quali permanga, sulla copia di documenti analogici originali unici, l'obbligo di autentica.
Nel marzo del 2006 il CNIPA pubblica anche il libro bianco del Ministero per l'Innovazione e le Tecnologie sulla dematerializzazione della documentazione amministrativa tramite supporto digitale. Nel testo si ipotizza che la gestione documentale pubblica costituisca il 2% del PIL e che un obiettivo di dematerializzazione del 10% possa generare, per ogni anno, un risparmio di 3 miliardi di euro! Nella medesima pubblicazione si evidenzia come nel corso del 2004 le sole Amministrazioni Centrali abbiano prodotto quasi 110 milioni di documenti, 160 milioni di registrazioni di protocollo e 147 milioni di documenti archiviati.
Una organizzazione pubblica o privata che vuole dotarsi di un sistema di conservazione documentale può decidere se delegare o meno il servizio di conservazione del proprio patrimonio informativo. Nel primo caso, la modalità di erogazione del servizio (acquisizione, conservazione, estrazione e fruizione, passaggio di

consegne verso altro gestore) e la durata contrattuale sono regolate attraverso un accordo, che nel caso di amministrazione pubblica passa per un processo di acquisizione (D.Lgs. vo 163/2006 e s.m.i.).
L'organizzazione che gestisce il servizio di conservazione documentale in un certo Paese deve operare nel pieno rispetto delle norme giuridiche di quel Paese. Per esempio, se tratta dati sensibili o soggetti a controllo da parte di altri Enti, come quelli fiscali o di bilancio, la protezione o la esigibilità di queste informazioni assume una rilevanza differente rispetto ad altre tipologie di dati.
Che questo argomento sia di interesse a livello non solo italiano lo testimonia il fatto che nell'ambito dello ISO[3] è in atto da alcuni anni un'attività di standardizzazione delle attività peculiari dell'archivistica. In Italia, poi, alcune regioni, in primis la Emilia Romagna con il suo progetto "*Polo Archivistico Regionale dell'Emilia - Romagna PAR-ER*", a cui stanno facendo seguito Toscana e Liguria, hanno attivato progetti di conservazione della documentazione degli enti pubblici nel proprio ambito regionale.
Nell'ambito del servizio di conservazione documentale non bisogna sottovalutare anche gli aspetti tecnici di sicurezza logica e fisica affinché si abbia la massima garanzia della conservazione integra del dato: se un conservatore collocasse il proprio data center all'interno di un locale umido oppure in un ambiente particolarmente polveroso o, anche, non attivasse gli opportuni controlli sull'accesso ai dati conservati, introdurrebbe inevitabilmente dei fattori di rischio.
Esistendo già delle norme internazionali nell'ambito della sicurezza (la famiglia ISO/IEC[4] 27000) e per la conservazione documentale (ETSI[5] TS 102 573[6]) è ragionevole orientarsi verso fornitori che abbiano processi interni certificati e che offrano la maggiore tutela rispetto alle caratteristiche tecniche correlate al servizio richiesto. Tuttavia, queste certificazioni non sono specifiche e, in assenza di ulteriori norme, la scelta del fornitore può ricadere - per un cliente non particolarmente esperto in questa materia - su quello che apparentemente sembra offrire il migliore rapporto costo/beneficio.
Le aziende europee che svolgono l'attività di conservazione dovrebbero operare nel rispetto dei requisiti sanciti dalla cosiddetta "Direttiva Servizi" (Direttiva Europea 2006/123/CE) recepita dall'Italia con il D.Lgs. n. 59 del 26 marzo 2010. La Direttiva 2006/123/CE, proprio per stabilire legami sempre più stretti tra Stati e popoli europei e creare uno spazio senza frontiere in cui sia assicurata la libera circolazione dei servizi, recita che gli Stati devono adottare misure (volonta-

3 ISO the International Organization for Standardization (www.iso.org).
4 IEC the International Electrotechnical Commission (www.iec.ch).
5 ETSI (European Telecommunications Standards Institute) è un Istituto di standard senza fini di lucro riconosciuto dalla Comunità europea che produce norme universalmente applicabili nel campo dell'ICT (www.etsi.org).
6 TS 102 573. Technical Specification. Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data for digital accounting.

rie) volte ad incoraggiare la qualità dei servizi stessi (art. 26 comma 1). La medesima Direttiva inoltre introduce il concetto di certificazione, rilasciata attraverso l'utilizzo di organismi certificatori e ordini professionali a livello Comunitario. Nel comma 5 del citato articolo 26 si richiede agli Stati membri, in collaborazione con la Commissione, di incoraggiare lo sviluppo di norme, sempre volontarie, intese ad agevolare la compatibilità fra servizi forniti da prestatori di Stati membri diversi e la qualità dei servizi.
Un recepimento puntuale di questo art. 26 della Direttiva 2006/123/CE, almeno per quanto riguarda i fornitori di servizi di conservazione digitale, è fornito dal sopra citato D.Lgs. 235/2010 con l'introduzione dell'articolo 44-bis che recita:
"44-*bis* (Conservatori accreditati). *1. I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza*, ***chiedono l'accreditamento presso DigitPA***.
2. Si applicano, in quanto compatibili, gli articoli 26, 27, 29, ad eccezione del comma 3, lettera a) e 31.
3. I soggetti privati di cui al comma 1 sono costituiti in società di capitali con capitale sociale non inferiore a euro 200.000."

In definitiva, quindi, ora esiste un dispositivo giuridico che, almeno limitatamente ai fornitori di servizi di conservazione digitale, introduce l'accreditamento facoltativo previsto dall'art. 26 della Direttiva 2006/123/CE relativo, specificamente, a "qualità e sicurezza". Non va, inoltre, trascurata l'importanza del comma 3 che, definendo un livello minimo di capitale, pone le basi per garantire che un fornitore di questi tipi di servizio disponga di solidità economica sufficiente ad assicurare l'indispensabile continuità di esercizio. Non resta, ora, che attendere i decreti tecnici attuativi.
Una volta instaurato l'accreditamento volontario per il fornitore, sia la Pubblica Amministrazione sia le organizzazioni private potrebbero utilizzarlo come criterio premiante, o addirittura discriminante, nella scelta del contraente per il servizio di conservazione documentale.
L'introduzione dell'art. 44-*bis* nel D. Lgs 82/2005 potrebbe coinvolgere il 95% delle aziende italiane con meno di 10 addetti[7], chiamate in un prossimo futuro a conservare in formato elettronico i propri dati. Esse potranno, come conseguenza, scegliere tra i servizi di conservazione quelli la cui affidabilità sarà stata certificata da DigitPA, cioè da un organismo sicuramente indipendente, oppure rivolgersi a fornitori esteri analogamente affidabili.
In effetti, l'obiettivo centrale della direttiva servizi è quello di incrementare la competitività del mercato dei servizi (anche quelli informatici) al fine di creare

7 Dato estratto dall'Istat dall'archivio statistico delle imprese Attive (ASIA) nel 2008.

nuova occupazione all'interno dell'Unione Europea. Infatti nella parte introduttiva, evidenzia la presenza di un elevato numero di ostacoli nel mercato interno che impedisce alle PMI (piccole e medie imprese) di espandersi oltre i confini nazionali e di sfruttare appieno il mercato unico. Sostiene inoltre che i servizi costituiscono il motore della crescita economica poiché rappresentano il 70% del PIL e che la frammentazione interna del mercato è dannosa per l'economia europea, in particolare per la competitività delle PMI, ed impedisce ai consumatori di avere accesso ad una maggiore scelta di servizi.
Con il citato articolo 44-*bis*, e con la emanazione dei decreti tecnici attuativi, si aprirebbe anche alle PMI italiane il mercato europeo della conservazione digitale al quale potrebbero rivolgersi per ottenere servizi affidabili. Va, però, anche considerato il vantaggio che il nuovo art. 44-*bis* del Codice dell'amministrazione digitale comporta per i fornitori di questi servizi: esso consente loro, mediante il riconoscimento da parte di DigitPA, di mettersi alla pari dei propri concorrenti europei, una volta "*certificate o valutate le loro attività da organismi indipendenti o accreditati*"[8], e competere a loro volta nel mercato europeo.

3. Standard internazionali

Attualmente esistono vari standard ISO che riguardano gli aspetti archivistici della conservazione documentale che definiscono la struttura e il formato dei metadati, in base ai quali indicizzare quanto conservato, e le modalità di realizzazione dei collegamenti tra i vari documenti, in modo da formare "fascicoli virtuali". Tra questi standard i più noti sono ISO 14721 Open Archival Information System (OAIS) e ISO 15489 Information and documentation - Records management.
L'obiettivo dello standard ISO 14721 è di fornire un quadro sia per la comprensione dei concetti archivistici necessari alla conservazione e all'accesso a lungo termine alle informazioni digitali, sia per regolare i rapporti tra chi crea e deposita i documenti e chi li utilizza.
Lo standard ISO 15489 indica come una organizzazione può mantenere i propri archivi in modo efficace e sistematico, realizzando un sistema documentale che supporti gli obiettivi di business dell'organizzazione stessa.
Altri standard in corso di sviluppo e definizione (tra cui ISO 14641, ISO 30300 e ISO 30301) insistono tutti principalmente sull'aspetto archivistico del tema.
Nessuno di essi, in altre parole, affronta il tema della sicurezza, limitandosi a rinviare, a tale riguardo, al rispetto della famiglia di standard ISO/IEC 27000. In assenza di adeguate indicazioni sulle misure di sicurezza informatica relative alla conservazione digitale il fruitore del servizio di digitalizzazione non avrebbe certezze riguardo l'affidabilità tecnica del fornitore ad espletare quel compito specifi-

8 Direttiva 2006/123/CE, art. 26, comma 1, lettera *a)*.

co. Per valutare l'importanza di tale affidabilità tecnica basti pensare all'ipotesi in cui, a causa dell'inadeguatezza delle misure messe in atto da un conservatore (ad esempio l'assenza di copie di sicurezza), il medesimo non riuscisse ad esibire al proprio cliente un determinato documento fiscale richiesto dall'Autorità durante un'ispezione. Nel citato caso, benché la perdita del dato dipenda dalla negligenza del conservatore, la responsabilità della mancata esibizione del documento all'Autorità richiedente, ricade totalmente sul suo malcapitato cliente.
Proprio per colmare questa lacuna nel giugno 2009 è stato costituito un gruppo di lavoro in UNINFO[9] con lo scopo di realizzare una specifica tecnica per la definizione di misure di sicurezza informatica per la conservazione documentale. Le fondamenta su cui si basa questo nuovo documento sono i già citati standard ovvero la famiglia ISO/IEC 27000 - Information Security Management System - e la specifica tecnica ETSI TS 102 573.

4. La proposta italiana UNINFO

Al gruppo di lavoro UNINFO hanno partecipato, oltre ad INAIL e DigitPA, i principali attori del mercato, ovvero aziende che forniscono servizi di conservazione, auditor, organismi governativi, il mondo bancario, esperti di sicurezza e di giurisprudenza informatica.
Proprio per renderne più semplice l'applicabilità, il documento di specifica tecnica è strutturato in modo da rivolgersi a due distinti attori: chi realizza ed eroga il servizio di conservazione e chi ha il compito di verificare la conformità del fornitore ai requisiti previsti dalla specifica (auditor) .
All'interno del documento le misure di sicurezza possono essere caratterizzate da tre livelli di applicabilità: obbligatoria, raccomandata e opzionale.
A chi imposta e gestisce il servizio di conservazione è richiesto inoltre di indicare in un documento ("*Statement of applicability*") le motivazioni di una eventuale mancata attuazione di alcuni requisiti oltre alle indicazioni dell'adozione di norme relative a documenti diversi dalle specifiche citate.
Per ogni capitolo del documento si riportano, inoltre, espliciti riferimenti a norme giuridiche italiane ed europee di interesse per la tematica trattata.
Al momento in cui il presente articolo è redatto il documento è stato già esaminato dai soci UNINFO ed è sottoposto alla procedura di approvazione da parte di UNI[10] come "Norma UNI". La conclusione di questa ultima fase procedurale - che inizia con un periodo di due mesi di inchiesta pubblica - è condizionata dalle date delle riunioni della Commissione Centrale Tecnica. È da ritenersi ragionevole che il documento possa essere sottoposto all'esame di detta Commissione nella prima riunione del 2011.

9 UNINFO è l'Ente di formazione federato all'UNI che promuove e partecipa allo sviluppo della normativa nel settore delle tecniche informatiche (www.uninfo.polito.it).
10 Cfr. UNI è l'Ente Nazionale Italiano di Unificazione (www.uni.com).

5. La nuova iniziativa ISO

Ormai è generalmente sentita l'esigenza di pubblicare specifiche tecniche di sicurezza informatica da mettere a disposizione di chi utilizza un sistema di conservazione digitale delle informazioni. Ne è riprova il fatto che recentemente (08/10/2010) il Joint Technical Commission JTC 1/SC 27 dello ISO ha lanciato un'iniziativa, denominata "Storage Security", che dovrebbe concludersi nel 2014, per stabilire le misure di sicurezza informatica relative alla sicurezza dei supporti informatici. L'ambito di tale iniziativa è ancora da definire in dettaglio.

6. Conclusioni

A ulteriore conferma circa il problema della mancanza di norme adeguate nell'ambito delle sicurezza documentale, la Commissione Europea già nel 2009 ha finanziato l'European Telecommunications Standards Institute (ETSI) per la realizzazione di un progetto di standardizzazione analogo a quello di UNINFO. ETSI ha avviato questo progetto il 15 marzo 2010, con la costituzione di una Specialist Task Force (STF) che ha preso spunto dal documento UNINFO. La differenza principale delle specifiche ETSI è la suddivisione del documento UNINFO in due parti. La prima, di tipo normativo, è rivolta a chi realizza e gestisce un sistema di conservazione a lungo termine. La seconda fornisce raccomandazioni a chi effettua ispezioni di auditing su tali sistemi. I documenti di questa iniziativa ETSI saranno pubblicati entro giugno 2011.
Non resta ora che attendere l'emanazione del decreto del Presidente del Consiglio dei Ministri previsto all'art. 71 del Codice dell'Amministrazione Digitale che definisca le apposite regole tecniche previste all'art. 20, comma 3 del medesimo codice. Questo Decreto, che finalmente aggiornerebbe la deliberazione CNIPA n. 11 del 19 febbraio 2004, potrebbe riferirsi o alla citata norma UNI o alla specifica ETSI onde indicare ai fornitori dei servizi di conservazione digitale le misure di sicurezza informatica da utilizzare.
La partecipazione a questi gruppi di lavoro ha avuto una duplice valenza: da un lato ha permesso la diffusione del *knowhow* tra le organizzazioni, pubbliche e private, che hanno aderito all'iniziativa e, dall'altro, ha consentito la realizzazione di documenti condivisi da cui sarà possibile estrarre requisiti tecnici da inserire nei capitolati o nei contratti di affidamento.

RIASSUNTO

Sebbene la tecnologia abbia fatto passi da gigante nell'ambito dell'archiviazione digitale delle informazioni, lo stesso non si può affermare rispetto alla integrità nel tempo della conservazione dei dati. Esistono ancora molte problematiche tecnologiche e normative che devono essere esplorate e definite. L'Istituto ha partecipato insieme con DigitPA ad un gruppo di lavoro interdisciplinare per redigere una proposta di norma per UNINFO, l'Ente di normazione federato dell'UNI per le tecnologie informatiche. La Commissione Europea, concordando sull'importanza della questione, ha finanziato nel 2009 un analogo progetto di standardizzazione, proposto e gestito da ETSI, che ha preso spunto dal lavoro di UNINFO, e che dovrà concludersi entro giugno 2011. Infine, anche ISO ha lanciato in ottobre 2010 un'iniziativa in un'area contigua la cui conclusione è prevista entro il 2014.
La pubblicazione delle citate norme UNI ed ETSI permetterà oltre alla definizione di criteri univoci nel processo di digitalizzazione e conservazione delle informazioni - attività peraltro strategiche per la PA italiana (Piano e-Gov 2012) - la scelta del fornitore orientata all'incremento della qualità mediante lo strumento della certificazione.

SUMMARY

The technology has made huge steps in the digital information archival, but the same assertion is not equally true as regards the reliable (i.e. ensuring integrity to) long term information preservation. A number of technologic and normative issues are still to be investigated in depth and implemented. INAIL participated, along with DigitPA, governmental body for the ICT (Information and Communication Technology), to a cross-disciplinary Work Group appointed by UNINFO with the purpose of developing a proposal for a standard in the long term information preservation domain. The EU Commission, agreeing on the importance of the issue, has in 2009 funded a similar standardisation project proposed and managed by ETSI, that is largely based on the UNINFO outcomes, and that is expected to be finalised by June 2011. Eventually, ISO too launched in October 2010 an initiative, in a contiguous domain, planned to be concluded in 2014.
Once published, the above mentioned specifications and standards issued by UNI, ETSI, ISO will provide a set of common criteria against which the information digitalisation and preservation process could be evaluated. This evaluation or, better, certification will allow users to make a learned choice of the service provider. Among such users the Italian Public Administrations will greatly benefit from this criteria to bolster their strategic goal of pursuing a high quality digitalisation, more in detail as regards the so called "Piano e-Gov 2012".