Ratifica della Convenzione di Budapest sul cybercrime e conservazione digitale dei documenti
ovvero la corretta formazione, gestione e conservazione delle informazioni rilevanti a garanzia del futuro della Società dell'Informazione

di Andrea Lisi (•)

Qualche tempo fa, nella prefazione di un mio recente volume[1] scrivevo:
"Ogni cultura ha avuto il suo materiale sul quale scrivere, ma è proprio la carta a costituire il principale strumento di conservazione della civiltà moderna e molto spesso ha dovuto resistere a guerre, devastazioni e soprattutto incendi per tramandare, con il suo misterioso profumo, la conoscenza e la memoria della nostra società.
È opportuno sottolineare al lettore che, se anche il libro può considerarsi il migliore strumento di trasmissione e di archiviazione delle informazioni, ai fini della conservazione nel tempo della nostra civiltà è stata determinante l'opera di copiatura dei manoscritti e degli stessi libri da parte di monaci, che hanno impedito la perdita di *dati* grazie appunto alle loro infaticabili opere di continuo *back-up*.
Oggi i cittadini dell'*Information Society* utilizzano una nuova tipologia di documento che ha ormai preso il sopravvento: il documento informatico.
La grande rivoluzione é iniziata con l'arrivo del *computer* e la sua capacità di trasformare qualsiasi informazione, testo, immagine o suono in un'interminabile sequenza binaria che può essere trasferita su diversi supporti di archiviazione in continua evoluzione tecnologica.
Il documento ha, così, perso per strada il peso della carta, per vivere una sua storia virtuale che lo lascia trasferire da un pc ad un altro, da un server a un altro, da un supporto a un altro.
Il documento informatico, infatti, vive a prescindere dal supporto che lo contiene, perchè nell'era dell'*Homo Digitalis* - in pochi istanti dettati dalla digitazione di un tasto - è possibile trasmettere, attraverso i confini indefiniti del "ciberspazio", conoscenze e informazioni straordinarie.
È il documento che cambia, dunque, salutando "dai paesi di domani"[2] i tradizionali concetti di originale e copia, di sottoscrizione e imputabilità. E, quando è il concetto stesso di documento a cambiare, allora inevitabilmente si modifica il suo processo di conservazione nel tempo".

(•)L'Avv. Andrea Lisi è Professore a contratto - Cattedra Informatica Giuridica, Facoltà Giurisprudenza - presso Università del Salento e Presidente di ANORC (Associazione Nazionale Responsabili della Conservazione Sostitutiva – www.anorc.it). Attualmente è il Coordinatore del Digital&Law Department Studio Legale Lisi – www.studiolegalelisi.it.
[1] *Conservazione dei documenti informatici*, a cura di Andrea Lisi, Edizioni CieRre, 2007, pp. 16-17.
[2] "Ti saluto dai paesi di domani, che sono visioni di anime contadine, in volo per il mondo" (di Fabrizio De Andrè, dalla canzone "Anime Salve", tratta dall'omonimo album, 1996, BMG Ricordi S.p.A.)

E' il documento, dunque, che cambia e diviene sempre di più per l'impresa e la PA informazione digitale giuridicamente rilevante da formare correttamente, da trasmettere con sicurezza, da archiviare e conservare con logiche e tecniche nuove che garantiscano la persistenza nel tempo della memoria digitale. Mai come adesso appaiono lungimiranti le parole del Prof. Renato Borruso secondo il quale: *il flusso degli elettroni nel computer è il nuovo inchiostro, i bit il nuovo alfabeto e la memoria della macchina la nuova carta…*

Il documento informatico è oggi *la rappresentazione informatica* ("sottoscritta" o "non sottoscritta") *di atti, fatti o dati giuridicamente rilevanti*[3]. Secondo questa definizione, l'informazione rilevante nel mondo digitale non è la "carta virtuale" e non è neppure la "scrittura telematica". Questi concetti sono culturalmente superati e sono teoricamente obsoleti e, pertanto, possono fuorviare noi giuristi nell'elaborazione dottrinale della nuova nozione di documento nella Società dell'Informazione. Il concetto di documento informatico non può non considerare cosa si intenda oggi culturalmente, sociologicamente e "tecnologicamente" come informazione rilevante in una realtà strategicamente orientata verso una gestione digitale dei propri dati.

Più correttamente il documento digitale / informazione rilevante viene a coincidere con: *testi, immagini, dati strutturati, disegni, programmi, filmati formati tramite una grandezza fisica che assume valori binari, ottenuti attraverso un processo di elaborazione elettronica, di cui sia identificabile l'origine* (art. 1 lett. d) D.M.E.F. 23 gennaio 2004 - Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto). Il documento digitale rilevante giuridicamente viene a coincidere così con qualsiasi dichiarazione di scienza o di volontà di cui sia conservabile nel tempo la memoria e sia verificabile la paternità/imputabilità giuridica.

Alla luce di queste considerazioni, il brocardo latino "*verba volant, scripta manent*" deve essere reinterpretato nel mondo digitale, dove qualsiasi informazione (a prescindere dalla forma di comunicazione della stessa) può essere attribuibile a qualcuno in modo ragionevolmente certo e può essere correttamente conservata nel tempo, attraverso l'applicazione di metodi corretti di sicurezza informatica e di memorizzazione delle informazioni rilevanti, in linea con la normativa italiana..

[3] Da ultimo, anche dal punto di vista penalistico il concetto di documento si allinea (finalmente!) a quello elaborato più di dieci anni or sono dalla normativa amministrativa e civilistica, liberandosi del peso (anacronistico) del supporto. Infatti, con la ormai completata (dopo soli sei anni!) ratifica della Convenzione di Budapest sulla criminalità informatica (Legge 18 marzo 2008 n. 48), viene abrogata la nozione di documento informatico contenuta nel art. 491 bis cod. pen. - *per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.*

Il giurista non può non confrontarsi con i recenti valori e le nuove certezze della società digitalizzata, dove la gestione dell'informazione costituisce il fattore determinante di successo per qualsiasi strategia di mercato. L'attento "giurista informatico" deve necessariamente applicare una adeguata e flessibile lente interpretativa al concetto di documento, alla sua gestione, trasmissione, memorizzazione su idonei supporti, archiviazione e conservazione nel tempo: è una sfida difficile, quasi impossibile per chi è nato con il peso della carta, ma non possiamo esimerci dall'affrontarla e non pensare così di far evolvere il concetto di documento, immaginandolo come qualcosa di profondamente, radicalmente diverso dalla rappresentazione digitale della "carta" e dello "scritto". E' una sfida che riguarda da una parte l'evoluzione normativa e dall'altra l'interpretazione corretta di una realtà che sta cambiando in modo improvviso e imprevedibile.

Fatte queste doverose premesse, risulterà agevole percepire come la scommessa del futuro digitale debba essere quella di garantire:
- la ragionevolmente certa paternità,
- la corretta trasmissibilità,
- la sopravvivenza nel tempo,
a tutti i dati digitali che abbiano un rilievo giuridico attraverso avanzate tecniche di sicurezza informatica.

La normativa italiana attualmente in vigore in materia di formazione, trasmissione e conservazione del documento informatico[4], si è data proprio il preciso compito di regolamentare tecniche idonee a conferire garanzia e stabilità alle informazioni digitali rilevanti e così deve essere interpretata nella sua complessità; tant'è che l'art. 44 del Codice dell'amministrazione digitale precisa che qualsiasi sistema di conservazione di documenti informatici deve garantire:
a) l'identificazione certa del soggetto che ha formato il documento (…);
b) l'integrità del documento;

[4] Dal punto di vista civile e fiscale, le norme principali in materia sono:
- il Codice dell'amministrazione digitale (Decreto legislativo 5 marzo 2005, n. 82): artt. 20-23 e artt. 40-44.
- il DPCM 13 gennaio 2004 "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici";
- il Decreto del Ministro dell'economia e delle finanze 23 gennaio 2004 (qui di seguito DMEF) "Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto";
- la Deliberazione CNIPA n. 11/2004 del 19 febbraio 2004 con le Note esplicative "Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali".
A queste norme devono essere aggiunti il D. Lgs. 20 febbraio 2004 n. 52 (di attuazione della direttiva 2001/115/CE, in tema di fatturazione elettronica) e il D. Lgs. 196/2003 sulla protezione dei dati personali, in particolare l'allegato B) dello stesso (richiamato dall'art. 44 del CAD) e il DPR 11 febbraio 2005 n. 68 (in materia di Posta Elettronica Certificata).

c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;
d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in Allegato B a tale decreto.

Oggi per qualsiasi impresa e pubblica amministrazione diventa non soltanto possibile "dematerializzare" (o più correttamente "digitalizzare") le proprie "informazioni di qualità" (dai documenti contrattuali a quelli contabili, sino a tutte le informazioni "sensibili" quali log file di navigazione, dati inerenti ai sistemi di videosorveglianza, documenti di lavoro, documenti privacy, e-mail e così via), ma risulta indispensabile procedere a "norma di legge" secondo strumenti e logiche di corretta formazione, sicurezza, stabilizzazione e regolare conservazione dei dati rilevanti.
La necessità di gestire correttamente le proprie informazioni non è soltanto determinata da un vantaggio economico e da un fattore di sicurezza, ma anche e soprattutto dal rischio concreto che il "documento informatico" prodotto a proprio favore non venga riconosciuto valido e rilevante in un qualsiasi procedimento giudiziale, se non è stato correttamente formato e conservato[5]! E nessuna società o ente oggi si può permettere di perdere informazioni rilevanti e soprattutto di non poterle utilizzare a proprio favore in un eventuale procedimento giudiziale!

Queste considerazioni risultano rafforzate dalla recente ratifica nel nostro ordinamento della Convenzione di Budapest[6] sulla criminalità informatica la quale opererà di fatto un'estensione per gli illeciti informatici della responsabilità amministrativa degli enti e delle società[7]
Per qualsiasi persona giuridica risulterà indispensabile, pertanto, predisporre una corretta e controllata gestione e organizzazione delle informazioni rilevanti in un preciso organigramma di

[5] Si ricordano, a titolo di esempio, alcune recenti pronunce giudiziali in materia:
- *nullità dei contratti di trading on line privi di firma digitale seppur siglati in area riservata e previa sottoscrizione di condizioni generali di servizio da parte di istituto di credito e investitore (perché manca la forma scritta)* – così Tribunale di Ravenna sent. 19 novembre 2007
- *Copia di pagina web su supporto cartaceo che non risulti essere stata raccolta con garanzie di rispondenza all'originale e di riferibilità a un ben individuato momento - qualificabilità come documento - non sussiste* – così Cass. Sez. Lavoro Sent. 02912/04
- *Acquisizione di file di log da parte della PG tramite mera consegna dei dati da parte dell'ISP – obbligo di verifica circa le modalità della conservazione degli stessi allo scopo di assicurare la genuinità e l'attendibilità nel tempo – necessità – sussiste* - Sentenza Tribunale Chieti n. 175/05.

[6] Come già ricordato, l'Italia con la Legge 18 marzo 2008 n. 48 ha finalmente ratificato la Convenzione del Consiglio dell'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001.

[7] Sulla convenzione di Budapest si consiglia la lettura di: *Sicurezza aziendale e risk management. Nuove strategie per evitare il cybercrime*, articolo di Annalisa Spedicato pubblicato su ScintLex alla pagina http://www.scintlex.it/notizia/328/76.html; *Criminalità informatica "senza frontiere": Budapest–Roma in soli 6 anni!* di Luigi Foglia pubblicato su ScintLex alla pagina http://www.scintlex.it/notizia/324/176.html; *Commento alla legge di ratifica della Convenzione di Budapest* di Marco Cuniberti, Giovanni Battista Gallus, Francesco Paolo Micozzi, Stefano Aterno pubblicato sul sito del Circolo dei Giuristi Telematici alla pagina http://www.giuristitelematici.it/modules/bdnews/article.php?storyid=1353.

ruoli e responsabilità al proprio interno e verso l'esterno. Occorrerà inevitabilmente dotarsi di mezzi e procedimenti che permettano di evitare non solo la perdita di dati e informazioni importanti per l'azienda, ma anche e soprattutto la loro modifica o la loro alterazione, sviluppando strumenti di gestione di tali documenti e atti che permettano di mantenerne la stabilizzazione temporale e l'integrità complessiva e che diano la facoltà di risalire pacificamente al titolare del documento, rendendo così facilmente individuabile il legame tra soggetto responsabile e informazione rilevante. Tutto questo ovviamente nel rispetto della normativa italiana sul corretto trattamento dei dati e sulla corretta formazione e conservazione dei documenti informatici.

Sviluppare questi processi non è semplice e per molte realtà potrà risultare poco conveniente realizzarli al proprio interno; strategicamente sarà più naturale e opportuno affidare questa responsabilità all'esterno, attraverso forme di affidamento in outsourcing della sicurezza e della gestione e corretta conservazione degli archivi digitali contenenti le proprie informazioni rilevanti.

Per tali motivi, nell'immediato futuro della Società dell'Informazione credo che non si possa fare a meno di *terze parti fidate* che assicurino:
- la paternità e immodificabilità delle proprie informazioni rilevanti (dati contabili e fiscali, file di log generati dalle comunicazioni elettroniche, transazioni elettroniche etc.)
- la loro corretta trasmissione
- la loro conservazione nel tempo

secondo procedure sicure e certificate in linea con la normativa in vigore.

E il compito di noi giuristi sarà anche quello, difficilissimo e delicato, di regolamentare nel dettaglio processi così complessi e definirne ruoli e responsabilità in normative di settore e "micro-ordinamenti" contrattuali.