PUBBLICA AMMINISTRAZIONE 24

DIG.Eat 2016

Digital Wars: la vendetta dei bit

DIGITAL WARS LA VENDETTA DEI BIT

Maggio 2016

E-gov

GRUPPO 24 ORE

Sommario

Pensare in digitale

Andrea Lisi *

* *Presidente Anorc*

Anche quest'anno il DIG.Eat di Anorc riapre le porte a operatori, esperti e utenti del digitale per un momento di confronto obiettivo sulla situazione e sulle possibili vie di sviluppo dell'innovazione nel nostro Paese. D'altronde il **dialogo costruttivo** tra le parti è uno degli strumenti più efficaci per cercare di dare ordine a una **situazione complessa** come quella della digitalizzazione nel nostro Paese, caratterizzata ancora da forti disomogeneità, da sacche di arretratezza accanto a esempi di eccellenza e da forti resistenze ai nuovi processi, soprattutto (ma non solo) nel settore pubblico.

Gli interventi legislativi recenti

Quest'edizione, nella quale abbiamo voluto dedicare una maggiore attenzione al mercato, arriva dopo una **serie di provvedimenti normativi di settore** in cui, finalmente, le esigenze del mercato digitale sembrano, almeno apparentemente, essere state prese in considerazione anche dal legislatore: penso a iniziative normative quali il Foia, il nuovo Codice degli appalti, il nuovo Cad, sino ad arrivare all'attuazione di Spid o alle ultime novità del processo amministrativo telematico, il cui contenuto purtroppo non risulta sempre soddisfare aspettative e reali bisogni, come a dire: la volontà c'è (e questo è già qualcosa) ma non sempre dà luogo a risultati validi e funzionali. Va dato atto che nella recente richiesta delle Commissioni parlamentari competenti di ascoltare le osservazioni di Anorc e di altre associazioni di categoria in merito sia alle modifiche del Cad e sia al Foia (osservazioni, queste ultime, poi in buona parte assorbite nel parere finale) è da leggersi un segnale positivo del desiderio, da parte dei poteri centrali, di tenere in considerazione le opinioni di chi rappresenta le aziende e i professionisti che operano nel settore digitale, che hanno il polso della situazione e sanno bene quali sono le difficoltà da sciogliere.

Certo, il **punto debole di questi interventi legislativi** tende a essere sempre la **mancanza di coordinamento e omogeneità tra le norme**, come se a prevalere fosse la tendenza a considerare ogni singolo testo normativo come un'entità indipendente e non come la parte di un complesso insieme in cui esso deve confluire senza conflitti, nel pieno rispetto, innanzitutto, della normativa primaria. E infatti, ancora oggi, si leggono testi normativi che sembrano abbozzati piuttosto che definitivi e invece di richiamarsi l'un l'altro in modo sistematico, magari affidando i principi generali relativi ai processi di firma, ai modelli di comunicazione e ai sistemi di gestione documentale a un unico corpus (quello che dovrebbe essere il Codice dell'amministrazione digitale), continuano a ribadire l'ovvietà, ma corredandola di eccezioni. Un **atteggiamento schizofrenico**, quello del legislatore, che si ripete da anni e non accenna a terminare, anzi, nella foga di comunicare il digitale, se possibile, peggiora.

Le regole da seguire

Eppure, invece di ostinarsi a legiferare ancora, inseguendo inutilmente la tecnologia, basterebbe seguire poche regole:

- **semplificare e armonizzare** l'attuale normativa primaria sulla digitalizzazione, delegando a regole tecniche comuni (magari racchiuse in un unico e coordinato Testo unico) i dettagli della tecnologia e dell'attuazione dei singoli processi. Fare in modo che ci siano regole comuni per tutti i settori, senza pericolose eccezioni;
- **definire le competenze digitali** necessarie a presidiare i modelli e i processi finalizzati a rendere digitali le nostre pubbliche amministrazioni e le nostre imprese. Se non si formano dei buoni manager per la governance digitale non potranno mai mettersi davvero in discussione i resistenti (oserei dire davvero resilienti) burocrati della carta. Gestire la transizione al digitale implica, infatti, la definizione di profili professionali nuovi, richiede l'affidamento di ruoli e responsabilità stategici a professionisti in grado di comprendere le potenzialità delle soluzioni a disposizione, di promuovere il cambiamento e operare in modo autonomo e consapevole;
- **pensare in digitale**. Non ha senso far percorrere le strade del mondo analogico all'innovazione digitale. Per far questo occorre osservare cosa succede a livello internazionale, senza ostinarsi a studiare schemi e strumenti solo italiani e, soprattutto, è necessario rompere gli schemi e reinventarsi con coraggio, anche come professionisti. Occorre sporcarsi le mani in modo multidisciplinare e mettersi in discussione ogni giorno;
- infine non c'è trasparenza senza digitalizzazione come non c'è digitalizzazione senza sicurezza informatica. È un'unica

catena del valore digitale che comporta attenzione al dato, all'informazione, al documento dalla sua formazione alla sua aggregazione, dalla sua gestione alla sua eventuale comunicazione e/o pubblicazione sino alla sua conservazione.

Osservazioni finali

E poi **occorre iniziare**, senza pensare di dover fare tutto subito, per poi non far nulla. E per partire bene occorre **puntare alla qualità** (che è anche qualità del dato), senza pressappochismi. Del resto *"fare (bene!) le cose vecchie in modo nuovo: questa è l'innovazione"*, ci ricordava l'economista Joseph Alois Schumpeter. E noi non dobbiamo far altro che crederci, per una buona volta.

AL DIG.EAT 2016 SI PARLERÀ DI

App ed eCommerce - Una nuova speranza, ore 10.00 -11.30

Identità e firme - L'attacco dei cloni, ore 11.40-13.10

Compliance, conservazione e protezione dei dati - La minaccia Fantasma, ore 14.30-16.00

Contratti IT, Business intelligence e Big data - Il risveglio della forza, ore 16.15-17.45

L'identità digitale tra Spid e Regolamento eIDAS

Giovanni Manca *

** Socio onorario Anorc, consulente di dematerializzazione e sicurezza Ict*

L'identità digitale ha raggiunto i **vent'anni di esistenza**. I Pin fiscali e previdenziali hanno aperto l'epoca dei grandi servizi in linea sviluppati per cogliere nella pubblica amministrazione la prima diffusione di Internet. Oggi siamo a un atteso punto di svolta, il Pin ancora pienamente in vita ha ceduto un pò di spazio alla Carta nazionale dei servizi (Cns) e alla nuova Carta d'identità elettronica (Cie). La novità si chiama Sistema pubblico per la gestione dell'Identità digitale di cittadini e imprese (Spid) che **dal 15 marzo 2016** ha iniziato a distribuire le identità digitali tramite i tre gestori di identità accreditati. Questo progetto è senz'altro cruciale per un diffuso ed efficace accesso ai servizi in rete di PA e imprese tramite il cosiddetto Pin unico.

Vediamo in sintesi qual è la storia dell'**identità digitale nei servizi pubblici**.

Cenni storici

Il tema dell'identità digitale esordisce in modo significativo nell'**articolo 10 della legge n. 127/1997** dove si parla di carta d'identità su supporto magnetico. La spinta garantita dalla diffusione di Internet e dalla conseguente messa in opera dei portali fiscali e previdenziali porta peraltro a una diffusione della password associata al codice fiscale dell'utente denominata Pin.

Il **Pin** è dedicato al servizio e consente l'accesso solo al portale dell'amministrazione emettitrice.

La disponibilità dei fondi Umts e i conseguenti finanziamenti per il cosiddetto e-government fanno nascere la **Carta nazionale dei servizi** (Cns). Il messaggio politico dell'allora ministro dell'innovazione Lucio Stanca era quello che non avesse senso disporre di servizi online **senza uno strumento unificato d'accesso** e che la diffusione della Cie nel 2002 risultasse ancora molto bassa. Con un'emissione attiva in circa 130 comuni. La Cns si diffonde in modo rapido in Lombardia, associata ai servizi socio-sanitari, ma il suo **utilizzo** è **estremamente limitato** a causa dell'indisponibilità presso i cittadini degli indispensabili lettori di smart card.

Qualche anno dopo, per omogeneità di scopo, alla Cns si associa la **Tessera sanitaria** (Ts), nata per sostituire il tesserino del Codice fiscale (Cf) e gestire il monitoraggio della spesa sanitaria. **Nasce la Ts-Cns** e i progetti, da esclusivamente regionali, diventano progetti cofinanziati dal Mef per la parte Ts e quindi legati a specifiche convenzioni tra lo stesso e le Regioni.

Alla data odierna la Ts-Cns è **diffusa per circa 40 milioni di unità**. L'utilizzo reale è a macchia di leopardo con aree geografiche dove addirittura il microchip è inutilizzabile per la mancanza della procedura di rilascio del Pin o per l'assenza di significativi servizi online.

Nel frattempo, la seconda fase della sperimentazione della Carta d'identità elettronica (**Cie**) ha raggiunto a oggi **13 anni di vita**, il progetto 17 anni, con una diffusione del documento pari a circa un cittadino su venti. Alla data è anche necessario sottolineare che la Cie è inutilizzabile per l'accesso ai servizi in rete a causa dell'assenza di adeguate infrastrutture di supporto al ciclo di vita del documento elettronico.

La **Ts-Cns** sta completando un **ulteriore ciclo di vita di 6 anni** e la Consip ha aggiudicato una gara per ulteriori 57 milioni di Cns da distribuire in sostituzione di quelle che scadono dopo aver esaurito il loro periodo di validità di 6 anni.

Stato dell'arte

Il Governo, come è noto, ha tra i sui **principali obiettivi di digitalizzazione** lo Spid. Questo sistema genera il meccanismo virtuoso di "una credenziale di accesso - un livello di accesso (i livelli sono tre) - tutti i servizi accessibili".

Lo Spid si affianca alla Ts-Cns e alla Cie (facciamo riferimento alla nuova versione) e l'ulteriore diffusione numerica della Ts-Cns crea una duplicazione di credenziali che è opportuno gestire.

Alla data del 15 aprile 2016 il sito dell'AgID (www.agid.gov.it) comunica che **in ambito Spid** vi sono:

- Amministrazioni attive: 7;
- Gestori dell'identità accreditati: 3;
- Servizi disponibili tramite Spid: 237;
- Identità Spid rilasciate: 24.800.

Sullo stesso sito viene presentato anche un **cronoprogramma sintetico** che porta al dicembre 2017. A questa data, tutta la pubblica amministrazione deve erogare servizi tramite Spid. Saranno ammessi accessi con la Cie e la Cns ma certamente il Pin rilasciato alla vecchia maniera non sarà più accettato.

Nel corso del 2016 inizierà a essere distribuita la **nuova Cie**, conforme alle specifiche tecniche del Passaporto elettronico ma in grado di gestire l'identità mediante meccanismi a radiofrequenza (contact less chip). La nuova Cie può interagire con i servizi in rete tramite uno smart phone dotato di interfaccia Nfc (sempre più diffusa). Questo consente di disporre di un lettore per la Cie senza che sia necessario comprarne uno ad hoc.

Ma nel frattempo si è incrementato il numero dei P**in** rilasciati in sede fiscale e previdenziale fino a superare i 25 milioni di credenziali in possesso di cittadini e professionisti. Se si considerano anche le credenziali rilasciate in modo settoriale per scopi specifici, possiamo ipotizzare oltre 40 milioni di codici distribuiti, tutti specifici per l'organizzazione che li ha rilasciati e i servizi che a essa fanno riferimento.

Il Regolamento eIDAS e l'identità digitale

Il Regolamento (Ue) **n. 910/2014** del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (noto anche come eIDAS) ha influenzato significativamente la storia dello Spid.

Nel Capo II dell'eIDAS si tratta dell'**identificazione elettronica e** del **suo possibile utilizzo** tramite il riconoscimento reciproco tra Stati membri e l'ammissibilità della notifica degli schemi di identificazione.

Spid è stato progettato in maniera da soddisfare i **requisiti comunitari**. I suoi livelli di garanzia per le credenziali sono coordinati con l'articolo 8 dell'eIDAS e con il Regolamento di esecuzione 2015/1502, che definisce le specifiche e le procedure tecniche minime che riguardano tali livelli.

Spid può essere notificato alla Commissione, assumendo conseguentemente il **profilo di identità comunitaria** per l'accesso ai servizi on line, da un organismo del settore pubblico.

Questa **possibilità transfrontaliera** arricchisce di contenuti Spid e spinge a una sua gestione proattiva e efficace.

Considerazioni finali

Giunti al momento di trarre qualche conclusione sull'identità digitale viene subito da chiedersi **se ci sono in cantiere proposte** di razionalizzazione e ottimizzazione delle varie credenziali di identità. Ma al momento la risposta non sembra positiva.

In ogni caso, al netto delle sempre presenti opinioni contrastanti (nel passato, ad esempio, sul perché fare la Cns invece di investire sulla Cie, ovvero produrre un documento unico con doppio microchip per Cie e Cns), la **spinta verso Spid è forte** e inevitabile.

Peraltro, il fatto che le pubbliche amministrazioni siano obbligate ad adeguare i loro servizi alle identità Spid dopo 24 mesi non aiuta la diffusione delle identità, considerato il lungo periodo di attesa.

È **indispensabile** che in questa fase storica le pubbliche amministrazioni colgano l'occasione per **definire** con il coordinamento di AgID **una tassonomia dei servizi erogati** che li classifichi sulla base del livello di garanzia delle credenziali richieste per l'accesso. Questa omissione ha creato una situazione di disomogeneità, perché ha consentito a erogatori diversi di una stessa tipologia di servizi la richiesta di requisiti diversi per consentire l'accesso. Altri temi, come l'eventuale costo per l'utente delle credenziali dopo il periodo di distribuzione gratuita, sono in fase di definizione.

Per la **diffusione nel settore privato di Spid** sarà importante definire l'onere economico che il fornitore di servizi deve sostenere per avere la verifica dell'identità da parte del gestore accreditato. Quest'ultimo tema è fondamentale, perché attraverso questo parametro di costo si definirà meglio il modello di business di Spid, ad oggi non perfettamente chiaro o definito.

Certamente aderire a Spid libera le pubbliche amministrazioni dal compito delicato e costoso della gestione del ciclo delle credenziali di accesso. Conseguentemente questo aspetto mette a disposizione risorse per la creazione di servizi sempre più efficaci per l'interazione via rete (anche in mobilità) con gli utenti.

Nello **schema del nuovo Cad**, alla data del presente documento, si rileva un possibile nuovo impulso per la diffusione dell'identità digitale. Infatti, nel nuovo **articolo 64-*bis*, comma 1** si stabilisce che: "*1. I soggetti di cui all'articolo 2, comma 2, rendono fruibili i propri servizi in rete, in conformità alle regole tecniche di cui all'articolo 71, tramite il Punto unico di accesso telematico attivato presso la Presidenza del Consiglio dei ministri senza nuovi o maggiori oneri per la finanza pubblica.*".

Si tratta del più volte annunciato **Italia Login**. L'**auspicio finale** è **che Spid sia valorizzato** con servizi reali, appetibili

per i cittadini, le imprese e i professionisti. Servizi tali da giustificare il costo, anche minimo, delle credenziali elettroniche. Tali servizi dovranno evitare veramente le code tramite il click. I servizi dovranno avere inoltre un **profilo moderno** basato su una **reale usabilità**, anche sui diffusissimi servizi in mobilità.

Si è iniziato un **nuovo percorso rivoluzionario**, si auspica che esso non si arresti o non rimanga inconcluso come gli altri tentativi visti nel passato.

Certo è che comunque la Cns continuerà a essere emessa (da contratto pubblico) per altri 5 anni e sarà valida per 6 anni dalla data di emissione: le **ultime Cns** dovrebbero scadere, quindi, nel **2027**. Nel frattempo Spid avrà compiuto i suoi primi 10 anni di vita e tanti milioni di nuove CIE saranno nelle tasche dei cittadini.

AL DIG.EAT 2016 SI PARLERÀ DI

L'identità digitale tra Spid e Regolamento eIDAS

Identità e firme - L'attacco dei cloni, ore 11.40-13.10

Un digitale che non cresce è un digitale che muore (come l'economia)

Mara Mucci *

** Camera dei Deputati*

Il *cambiamento*, soprattutto nel caso in cui si parli di digitale, non può prescindere da **due fasi**: quella operativa che fissa le regole e quella culturale che le applica. Talvolta serve che le norme forzino i comportamenti, viceversa capita che siano le azioni a richiedere nuovi paradigmi di attuazione. Così pretende il digitale. Non può esisterne una corretta applicazione senza una **struttura specifica**, delineata su misura per esaltarne le potenzialità. Affinché il matrimonio tra digitalizzazione e pubblica amministrazione funzioni, occorre dunque partire da queste due prerogative: **competenze e responsabilità**. Da qui deve dipanarsi la rete in grado di sostenere, agevolare e diffondere il verbo del codice binario.

Davanti allo stato attuale dell'informatizzazione dei servizi della PA, questo è il binomio su cui si sta concentrando Anorc, e che condivido interamente: **ripensare in digitale partendo dalle competenze.** "Ripensare", perché il digitale calato nella gestione della PA ne cambia la forma. "Competenze", perché per farlo servono generali che impostino il lavoro e soldati che lo applichino quotidianamente. In sintesi, formazione continua e responsabilità consapevole d'azione.

Oggi siamo invece davanti ad un Paese succube della cosiddetta **burocrazia difensiva**, che partendo da un'incapacità di assumersi responsabilità da parte di funzionari e dipendenti, culmina con un **rallentamento** - e in casi gravi anche blocco - **delle istituzioni**.

I dipendenti pubblici hanno paura a muoversi perché non sono consapevoli di ciò che possono e non possono fare, e delle conseguenze delle proprie azioni. In questo scenario, il **digitale** è **paradossalmente un problema in più**.

Anche per questo servono figure professionali idonee, dotate di pieni poteri organizzativi, in grado di comprendere le lacune di competenza e quelle di attribuzione dei compiti.

Profili professionali che si occupino di e-government dei flussi informativi e documentali, ed in grado di ripensare i processi. L'inquadratura di professioni operanti in ambito Ict deve affiancare un'importante opera di formazione dei dipendenti e dirigenti pubblici.

Esempi concreti

Il digitale è un **flusso continuo**, come i pensieri: se un passaggio, benché minimo, si inceppa, salta tutto il castello procedurale. Le regole devono dunque essere rispettate e gli interpreti formati a dovere. La **sovrapposizione attuale del digitale all'analogico** giustifica, invece, quell'inerzia della burocrazia che si ferma laddove manca un timbro, dove davanti ad un'incertezza corre a chiamare in causa l'assessore o il dirigente competente per dirimere la questione. In una **struttura pensata in digitale** questo non accade, le responsabilità di un malfunzionamento emergono in automatico ed i passaggi sono semplificati. "For dummies" per intenderci. L'informatica ha bisogno di strade certe che vadano dal punto A al punto B. Non comprende, a differenza della burocrazia, punti C.

Un altro esempio riguarda l'**interazione col mondo esterno**. La digitalizzazione dei processi non può essere confinata solo internamente all'amministrazione, ma deve necessariamente essere anche una **proiezione esterna**, la contaminazione di una rete di funzioni. All'interno della pubblica amministrazione, questo deve tradursi in un collegamento delle sue strutture sulla logica dell'informatizzazione. Procedure di dialogo che vanno impostate anche con le società partecipate o esterne cui l'ente pubblico si rivolge per garantire i suoi servizi.

In Italia sono diversi i comuni che si sono, ad esempio, appoggiati al digitale per gestire le segnalazioni dei cittadini su malfunzionamenti e guasti dei servizi pubblici. L'idea di un digitale che sostituisce l'analogico - una mail al posto di una lettera - deve essere affiancata da una riorganizzazione affinché il digitale metta in campo il suo potenziale. Così, l'archivio segnalazioni può diventare un protocollo di gestione degli interventi, un'interfaccia cui si rivolgono i vari uffici tecnici per valutare tipologie, tempi e case history delle procedure passate o in atto. Questo è un **approccio digitale** che oltre a velocizzare e rendere più accessibile un servizio, a cascata offre altre **numerose opportunità di semplificazione**. Per fare questo occorre schiantare gli attuali dogmi che sigillano a tenuta stagna i vari settori della PA, mettendoli in rete fra loro. Inoltre, questa procedura si ferma inesorabilmente quando l'ente pubblico si trova ad utilizzare gli stessi dati con una società esterna cui è appaltata la gestione di determinati servizi. Un esempio veloce: un sindaco che ha digitalizzato il sistema di segnalazione guasti, affiancandolo ad una procedura di comunicazione sui tempi di ripristino, come potrà

completare il servizio se non ha dialogo con l'ente terzo che esegue i lavori, e se quest'ultimo non aggiorna la pratica con i tempi di evasione? I sistemi informatici vanno dunque ragionati sia con la struttura interna della PA, sia con i protagonisti esterni del suo lavoro: società partecipate o indipendenti, cui gli enti pubblici si rivolgono.

Osservazioni conclusive

Rivedere i processi della pubblica amministrazione in chiave digitale non solo è importante, ma necessario. E lo è di più **mettere in condizione la PA e i suoi dipendenti tutti, di maneggiare ed utilizzare i nuovi strumenti** in modo consapevole, altrimenti saremo davanti a processi innovativi non sfruttati pienamente. Il risultato paradossalmente è quello di una maggiore lentezza e maggiori costi per la collettività.

Guardiamo quindi in modo alto non solo ad un approccio evolutivo nel senso digitale del termine, ma puntando sulle competenze. Sulle responsabilità e sulle figure professionali di riferimento. Senza questo passaggio necessario ci ritroveremo una PA non al passo con le aspettative di un pubblico sempre più nativo digitale. Ed il fattore che esplode in mano a chi amministra è tutto politico, si chiama **perdita di fiducia nei confronti di chi amministra**, si chiama senso di lontananza fra chi gestisce la cosa pubblica e chi ne beneficia, significa anche perdita di investimenti locali per eccessiva "burocrazia".

Almeno questa volta cerchiamo di affrontare un'esigenza senza partire dal fondo. Partiamo dalle competenze e dalle responsabilità di figure professionali chiare.

LA VOCE DEL MERCATO

**due chiacchiere con Pablo Pellegrini (SB Italia)
e Stefano Zanoli (Unimatica)**

In questi ultimi tempi siamo stati invasi da manifesti programmatici, per lo più politici, sulla digitalizzazione. Aldilà delle campagne promozionali del Governo, dal punto di vista del mercato e quindi dal punto di vista di un'azienda come la vostra, impegnata sui temi del digitale, qual è la reale sensazione? In quale direzione si sta muovendo la digitalizzazione in Italia?

Pablo Pellegrini, SB Italia:

SB Italia opera nel settore della digitalizzazione da molti anni e ha realizzato con la propria piattaforma Docsweb centinaia di progetti di dematerializzazione, di conservazione e gestione di Processi totalmente digitali.

Bisogna dire che negli ultimi anni la pubblica amministrazione e i governi hanno fatto della dematerializzazione un argomento sul quale pubblicizzare ma anche realizzare diverse iniziative.

A partire dalla normativa sulla conservazione sostitutiva fino all'introduzione della fattura elettronica alla PA bisogna dire che il Governo ha dato certamente un impulso allo sviluppo della digitalizzazione in Italia.

Se pensiamo a 10 anni fa si può dire che l'incremento di archivi digitali che sostituiscono a tutti gli effetti gli archivi cartacei è stato importante, questo cambiamento è anche culturale: oggi trovare un responsabile amministrativo che non conosca la conservazione sostitutiva e digitale risulta difficile.

La nuova sfida per le aziende italiane poggia su due temi: il processo digitale e l'interoperabilità digitale fra organizzazioni.

Su questi temi il mercato in Italia ha ancora molto da fare, soprattutto per le aziende medie e piccole che pare non riescano ancora ad apprezzare i vantaggi di queste soluzioni.

Operatori come SB Italia e Associazioni come Anorc svolgono un ruolo chiave nel consentire alle aziende di accedere a soluzioni di digitalizzazione dei processi e conservazione digitale dei documenti con investimenti sostenibili e utilizzando tecnologie evolute.

La chiave è lavorare i contenuti dei documenti in digitale fin dall'inizio e provvedere a rendere digitali processo e conservazione.

Stefano Zanoli, Unimatica

Unimatica opera esclusivamente su progetti inerenti la digitalizzazione. La domanda del mercato è in crescita. Unimatica dispone di una serie di prodotti e servizi in linea con i piani nazionali sul digitale.

Disponiamo di software per la firma grafometrica che vanta referenze importanti nel mercato bancario, assicurativo, retail ed utilities. Siamo stati i primi a realizzare con successo un progetto per la firma dei contratti bancari presso un grande banca e abbiamo fornito la firma in mobilità a un'importante rete di promotori finanziari.

Abbiamo inoltre realizzato un prodotto per i promotori finanziari con firma grafometrica in uso in una banca. Siamo attivi in 3.400 enti locali con l'ordinativo informatico e siamo Conservatori accreditati presso AgID, con oltre 700 milioni di documenti conservati.

Pensiamo che i processi digitali in Italia abbiano intrapreso una direzione corretta, e che vada sostenuta con azioni concrete da parte del legislatore.

Tante sono le novità in ambito legislativo: modifiche al Codice dell'amministrazione digitale, nuovo Regolamento europeo privacy, fatturazione elettronica… La normativa frena i processi aziendali oppure essere compliance può rappresentare un vantaggio per l'azienda?

Stefano Zanoli, Unimatica

La normativa, pensando alla fatturazione elettronica, al regolamento sulle firme elettroniche, e ad altre norme sulla conservazione del registro di protocollo, ha contribuito positivamente allo sviluppo di processi digitali nelle aziende e nella PA Italiana.

La fatturazione elettronica per i privati, sebbene non obbligatoria, potrà portare altri benefici per le aziende che intraprenderanno questa strada. La recente bozza di modifica del Codice dell'amministrazione digitale ha necessità di essere rivista con rigore.

Riteniamo che il regolamento eIDAS a livello europeo sia un passo importante verso servizi digitali efficaci.

Anche la Privacy va considerata come elemento chiave per tutelare i diritti delle persone e delle aziende.

Pensiamo che le norme siano necessarie per orientare le aziende che operano nel digitale a produrre e realizzare servizi professionali.

Pablo Pellegrini, SB Italia

La normativa va considerata secondo noi come una spinta alle aziende per introdurre soluzioni di digitalizzazione e dematerializzazione.

Il Codice dell'amministrazione digitale non introduce di fatto obblighi, ma opportunità per le aziende, e operatori come SB Italia e Anorc svolgono il loro ruolo per rendere applicabili e convenienti le soluzioni proposte dalla normativa.

Anche quando è stato introdotto un obbligo come la fattura elettronica alla PA - il cui scopo era quello di diffondere la pratica del documento informatico - le aziende hanno vissuto questo obbligo come un fardello senza ritorno di benefici. Tuttavia a distanza di un anno si sta comprendendo come lo scambio di documenti+dati fra aziende porti ad un notevole risparmio sui processi ed anche a migliori servizi, e si inizia a parlare insistentemente di fatturazione elettronica fra privati, al di là degli incentivi prospettati.

Ovviamente l'utilizzo di informazioni digitali ha coinvolto anche l'Organo di controllo della Privacy: tuttavia, ottemperare alle indicazioni ricevute fa parte del servizio di operatori come SB Italia e le aziende possono utilizzare le diverse soluzioni senza troppe difficoltà.

Complessivamente, quindi, le soluzioni proposte dalla normativa hanno portato opportunità e vantaggi per le aziende.

SB Italia e Unimatica aderiscono rispettivamente alle Associazioni Anorc e Aifag, in che termini la partecipazione e l'attività associativa possono supportare vision e mission aziendale?

Pablo Pellegrini, SB Italia

SB Italia segue Anorc fin dalla sua fondazione con una collaborazione attiva anche nel processo di divulgazione in merito agli argomenti relativi alla digitalizzazione.

Organizzazioni come Anorc e Aifag svolgono un ruolo essenziale che parte dalla corretta interpretazione del panorama normativo esistente: le associazioni costituiscono l'anello di congiunzione fra gli operatori come SB Italia e le istituzioni, per comunicare e apporre le necessarie correzioni fornendo una corretta interpretazione della normativa.

SB Italia spesso condivide la proposizione sul mercato delle soluzioni innovative anche con Anorc e i suoi esperti: le associazioni svolgono l'importante funzione di divulgazione ma anche ascolto del mercato e delle esigenze aziendali, facilitando il ruolo degli operatori e rendendo più chiaro il contesto agli utilizzatori.

Stefano Zanoli, Unimatica

Le associazioni Anorc ed Aifag svolgono un ruolo importante per garantire un dialogo con il legislatore che necessita di interlocutori qualificati provenienti dal settore digitale.

È un servizio importante, in quanto favorisce un processo di conoscenza effettiva tra gli operatori del settore e il legislatore.

Le due associazioni svolgono, inoltre, un'importante funzione di formazione sulla conservazione a norma e le firme elettroniche. In particolare, Aifag contribuisce attivamente per realizzare la interoperabilità dei sistemi di firma elettronica avanzata operanti in Italia.

Le aziende necessitano di una formazione e di una rappresentanza qualificata sul tema del digitale atta a favorire una trasformazione dei processi analogici, verso processi digitali.

Anorc svolge un ruolo importante di formazione degli utenti aziendali e della PA, ed inoltre è di stimolo per le aziende che operano nel settore della conservazione.

La conservazione in ambiente digitale: norme, modelli e azioni

Gianni Penzo Doria *

** Vice Presidente Anorc, Direttore generale Università degli Studi dell'Insubria*

La conservazione dei documenti in ambiente digitale rappresenta un **processo** particolarmente **complesso e proattivo**. Complesso, in quanto esistono una miriade di norme (italiane e internazionali) e di modelli concettuali da scegliere in relazione a numerose variabili. Proattivo perché, mentre la conservazione di un documento cartaceo si risolve nella maggioranza dei casi in un unico intervento di descrizione e di tutela di un bene sostanzialmente immutabile nel tempo, un documento digitale richiede, al contrario, una serie continua e ininterrotta di interventi. Quest'ultimi servono a garantire la conservazione nel tempo di un oggetto in grado di modificarsi continuamente. Anzi, proprio per poter essere conservato, deve mutare.

Da ciò consegue che la **cristallizzazione di un oggetto digitale** rappresenta **un assurdo dal punto di vista della conservazione**. È necessario, quindi, affrontare i passaggi nel tempo della tecnologia e del progresso. Ogni cambiamento, riferito a un nuovo applicativo, a un supporto innovativo, a un formato più flessibile, può mettere in crisi il concetto stesso di *preservation*. In buona sostanza, la conservazione è un processo continuo e ininterrotto per salvaguardare, non tanto il documento nella forma primigenia, quanto piuttosto il contenuto in forma affidabile e persistente nel tempo.

La conservazione come processo a sistema: la regola del conte

La conservazione dei documenti **non inerisce il documento in sé**, ma a una serie di elementi che lo caratterizzano e lo identificano in un contesto di produzione, di funzione, di interdipendenza con altri documenti. In altre parole, per conservare in maniera affidabile nel tempo un documento, non basta "congelarlo", perché l'ibernazione non appartiene al mondo digitale.

Risulta, invece, necessario esibire le prove di una **catena ininterrotta di attività e di custodia affidabile degli oggetti digitali** (la *chain of* preservation, come magistralmente illustrata da *Interpares* – www.interpares.org). Essa, infatti, riguarda un insieme di metadati e di azioni esplicitate attraverso le prove affidabili di una sequenza di responsabilità senza soluzioni di continuità.

Possiamo, pertanto, esemplificare la conservazione attraverso la **regola del conte**. In questo modo, tenteremo di sintetizzare il processo a sistema attraverso tre parole:

1. *conte*nuto;
2. *conte*nitore;
3. *conte*sto.

Infatti, oggi sappiamo che non è più possibile conservare il documento nella forma iniziale nella quale è stato prodotto. Ciò accade perché nel tempo il documento subisce una serie di attività di *traditio* da un supporto a un altro, da un formato a un altro e da una tecnologia a un'altra. Di conseguenza, risulta **possibile preservare soltanto il *contenuto* indipendente dalla rappresentazione**. E ciò con buona pace della diplomatica classica che, nella rappresentazione delle cose attraverso gli elementi estrinseci del documento (scrittura, inchiostro, supporto ecc.), ha basato per secoli alcune delle prove dell'autenticità.

Nella diplomatica digitale, invece, risulta **indispensabile anche un *contenitore*, affidabile ma mutevole** al tempo stesso, cioè uno o più formati in grado di poter rappresentare il documento oltre i confini dell'obsolescenza. Nel mondo digitale, infatti, il contenitore è destinato inevitabilmente a essere sostituito dall'evoluzione dei formati in grado di garantire, *in quel preciso momento e* - ragionevolmente - *per un periodo di tempo accettabile*, la rappresentazione affidabile.

Da ultimo, ogni documento deve essere **comprensibile in un *contesto* determinato**. Per queste ragioni, il processo di conservazione trascina con sé tutti gli elementi idonei alla contestualizzazione. Primi fra tutti, gli elementi di contesto funzionale (registrazione, classificazione e fascicolatura, a mente dell'articolo 44 del Dlgs n. 82/2005). Su queste basi, le **regole tecniche sulla conservazione**, contenute nel Dpcm 3 dicembre 2013, rappresentano uno spartiacque rispetto a tutta la normativa pregressa. Prima, infatti, l'oggetto da conservare era esclusivamente il documento nella sua solitaria essenzialità di monade, nella convinzione erronea che un immagazzinamento di bit (*storage*) sarebbe stato in grado sostituire la conservazione affidabile di un complesso di interrelazioni, di contesti e di documenti (*preservation*).

La normativa italiana

Ci abbiamo messo vent'anni (1993-2013), ma sembra che ne sia valsa la pena, tanto rivoluzionario è l'insieme delle **regole tecniche dell'amministrazione digitale**. A questo punto, possiamo affermare che, anche sotto il profilo normativo, il processo di conservazione è sintetizzabile come un **insieme di interrelazioni** tra:

1. Team della conservazione: composto da un archivista, un informatico e un addetto alla privacy;
2. Modello concettuale di riferimento;
3. Set di metadati (di ambito funzionale, operativo, tecnologico ecc.);
4. Formati idonei alla conservazione e alla disseminazione;
5. Piano per la sicurezza.

Il team della conservazione

L'articolo 44, comma 1-*bis*, del Dlgs n. 82/2005 recita: *"Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera 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"*.

Da ciò discende che il legislatore italiano ha previsto un **insieme di competenze dedicate** al processo di conservazione, in coalescenza interprofessionale. Nessun archivista, nessun informatico, nessun *privacy officer*, nella propria solitudine, potrebbe affrontare e sciogliere i nodi complessi della *digital preservation*. Tra questi, deve essere scelto - come prevede la normativa italiana - il ***Responsabile della conservazione***, con il compito di rapportarsi con il ***Conservatore* accreditato**, cioè un soggetto terzo in grado di garantire la conservazione affidabile nel tempo.

Il modello concettuale

Prima di tutto, il team deve scegliere il modello concettuale di riferimento. In virtù delle recenti regole tecniche sulla conservazione, contenute nel **Dpcm 3 dicembre 2013**, è stato meritoriamente imposto il **modello *Open archival information system - Oais***, come descritto nella norma ISO 14721.

A onor del vero, si tratta di un **modello internazionale**, sviluppato in seno alla Nasa, per la conservazione dei dati delle missioni spaziali. Tuttavia, essendo un modello "alto" e flessibile, può essere applicato anche alla conservazione di documenti digitali.

Il set di metadati

Il documento digitale, di norma, non è auto-consistente, né auto-esplicativo. Esso ha bisogno di una serie di **informazioni di corredo per essere** reso **identificabile, intellegibile e fruibile**. In Oais, per essere "comprensibile", deve essere associato alle informazioni in grado di esplicitare le procedure affidabili della propria rappresentazione. Ad esempio, l'autore, l'oggetto, il numero di registrazione, il soggetto produttore, gli elementi identificativi degli altri documenti interrelazionati all'interno di un'unità archivistica o di una serie (o, termine improprio, "aggregazione documentale"). In fin dei conti, il registro di protocollo e il sistema di conservazione altro non sono che un insieme complesso di descrittori di oggetti, cioè di metadati molto raffinati.

Essi possono essere ripartiti in **tre categorie**:

- Descrittivi: per facilitare il recupero e l'identificazione;
- Gestionali: per supportare la gestione;
- Strutturali: per interrelazionare fra loro risorse informative complesse.

I **metadati di riferimento** per il modello di conservazione secondo la normativa italiana sono descritti nell'allegato 5 al Dpcm 3 dicembre 2013.

I formati

Il formato è un sistema in grado di garantire la **modifica e** l'**intellegibilità di un file**. Con il progresso, abbiamo reso obsoleti formati utilizzati solo qualche anno fa. Inoltre, fattore fondamentale per il nostro discorso, non tutti i formati sono idonei alla conservazione a lungo termine. Parimenti, non tutti i formati idonei alla conservazione sono efficaci per la disseminazione e per la diffusione a una pluralità indistinta di soggetti potenzialmente interessati (si pensi, ad esempio,

alla pubblicità legale online). Da ciò deriva che ogni formato scelto per la conservazione in un momento e in un contesto determinato rappresenta la scelta – migliore e ponderata – in *quel* momento e in *quel* contesto. Mutando **tempo e condizione**, probabilmente la scelta del formato risulterebbe differente.

Per queste ragioni, le parole **migrazione e conversione** sono intrinseche alla conservazione e **attengono principalmente ai formati**. Sostanzialmente, non conosciamo i formati del futuro, ma oggi dobbiamo essere in grado di sceglierne alcuni, non uno soltanto, cui affidare il viaggio ininterrotto di un documento nel tempo e nello spazio. Inoltre, per garantire l'efficienza del sistema di conservazione, risulta indispensabile scegliere tra quelli meno votati all'obsolescenza rapida. Sono questi i motivi che spingono un conservatore a scegliere formati aperti, non proprietari, idonei all'interoperabilità, largamente adottati, indipendenti da architetture hardware e software e autoesplicativi. La cosa è ben nota al legislatore italiano che, pur tra qualche incertezza, se ne occupa da almeno vent'anni.[1]

I **formati di riferimento** per il modello di conservazione secondo la normativa italiana sono descritti nell'**allegato 2 al Dpcm 3 dicembre 2013**, ma sono in aggiornamento costante sul sito web istituzionale dell'Agenzia per l'Italia digitale.

La sicurezza

Sgombriamo ora il campo da un equivoco. I sistemi sicuri non esistono, ma **esiste un livello di sicurezza ragionevolmente accettabile** come misura minima per poter garantire nel tempo la *traditio memoriae*. La sicurezza, intesa nella sua più ampia accezione, infatti, è uno dei pilastri della conservazione. Anzi, **senza sicurezza non può esservi conservazione affidabile**. Ciò vale sia per il mondo tradizionale sia per il mondo digitale.

Probabilmente potremmo arrivare a dire che la conservazione digitale, per molti aspetti, coincide con l'applicazione delle misure minime di sicurezza. Esse riguardano i locali, gli accessi, la tracciabilità, i sistemi hardware e software con l'**obiettivo di ridurre i rischi e limitare gli eventuali danni** partendo proprio dalla consapevolezza che ciò possa avvenire.

Conclusioni provvisorie

La conservazione digitale è un processo che richiede almeno **due requisiti fondamentali**: un'altissima qualificazione professionale degli attori coinvolti e una terzietà rispetto al soggetto produttore.

Partiamo da quest'ultima affermazione. Nella normativa italiana, l'archivio storico è stato concettualizzato, appunto, come *separata sezione d'archivio* (Dpr n. 1409/1963), cioè affidato alla tutela di personale differente rispetto a chi lo aveva prodotto. Si presume, dunque, che quest'ultimo non avrebbe interesse a sopprimere, a occultare o a modificare i documenti non prodotti direttamente. A questa **terzietà** si è ispirato anche il legislatore più recente, affidando il registro giornaliero di protocollo al sistema di conservazione, in quanto terzo, anche se non ultroneo, rispetto al corrente. Riguardo alla qualificazione professionale, l'esperienza dimostra che soltanto in casi sparuti gli archivi sono stati affidati alle cure di archivisti. Anzi, l'archivio in sé, nella concezione imperante e sciatta, è un luogo - non una funzione - in cui la professionalità degli operatori non è nemmeno presa in considerazione. I tempi, però, stanno cambiando.

Il **futuro digitale**, a mio avviso, è nelle mani dei **conservatori accreditati**, siano essi poli di amministrazioni pubbliche o soggetti privati. Essi hanno l'obiettivo di investire continuamente e per *default* in formazione professionale in grado di viaggiare sullo stesso binario e alla stessa velocità del progresso. Il mondo ha bisogno di *cyberarchivist*, di *privacy officer* e di *Ict* al passo con l'evoluzione dei sistemi documentali e in costante interrelazione fra loro. Difficilmente le amministrazioni pubbliche e le imprese saranno in grado di investire un così alto numero di risorse umane e finanziare in progetti tanto ambiziosi. In fin dei conti, rendere il passato al presente con una proiezione sul futuro non è cosa che tutti possono permettersi.

AL DIG.EAT 2016 SI PARLERÀ DI

La conservazione in ambiente digitale: norme, modelli e azioni
Compliance, conservazione e protezione dei dati – La minaccia Fantasma, ore 14.30-16.00

[1] *Ad esempio, Aipa, delibera 30 luglio 1998, n. 42, art. 6; Dpcm 31 ottobre 2000, art. 16; Dpcm 30 marzo 2009, art. 40. Anche la normativa italiana sul tema, fatto di per sé non esaltante, è soggetta a rapida obsolescenza, tanto che le tre norme appena citate sono tutte abrogate. Il motivo è semplice e disarmante: la norma è neutrale rispetto alla tecnologia. Di contro, quando si avventura a ingabbiare il progresso, esce in Gazzetta ufficiale già obsoleta.*

Smart contracts e sistemi di blockchain: quale regolamentazione?

Sarah Ungaro

* *Digital&Law Department (Studio legale Lisi)*

L'utilizzo dei big data e dei sistemi alla base dell'Internet of Things (IoT) ci pone oggi moltissime opportunità, ma anche **nuove questioni giuridiche**: sicurezza, tutela della privacy, proprietà dei dati e possibilità di utilizzo da parte di terzi sono infatti aspetti da non sottovalutare quando si affrontano le tematiche della relativa contrattualizzazione e regolamentazione.

Smart contracts

Tuttavia, sebbene sia possibile cogliere intuitivamente l'importanza di tali profili, non è altrettanto immediata la correlazione tra la gestione delle informazioni ricavabili dalla c.d. big data analytics e dall'utilizzo di sistemi di IoT con alcuni degli elementi che accompagnano l'avvento (ma ormai, la diffusione) dei c.d. smart contracts e dei sistemi di blockchain, questi ultimi di estremo interesse soprattutto per l'ambito bancario e finanziario.

Ma **cosa si intende** quando si parla di smart contracts o di blockchain e quali sono le più importanti problematiche giuridiche (e di regolamentazione, non solo contrattuale, ma anche normativa) che ci attendono all'orizzonte?

Di seguito si cercherà di tracciare le caratteristiche essenziali alla base di tali sistemi, che risulta indispensabile provare a comprendere per individuare **quali possano essere i profili di criticità** di cui tener conto in fase di contrattualizzazione e di regolamentazione dell'utilizzo degli stessi.

Di **smart contracts**, in realtà, si parla fin dagli anni '70, ma solo ora se ne stanno studiando le applicazioni concrete in diversi ambiti, anche grazie alle potenzialità offerte dal legame di tali sistemi con la tecnologia blockchain. Nello specifico, gli smart contracts non sono altro che **contratti tradotti in un linguaggio di programmazione**, quindi in un codice eseguibile da un sistema informatico, che dunque si auto-eseguono, applicando in modo automatico le clausole della negoziazione che è stata stabilita, senza l'intervento né delle parti, né di un soggetto esterno. Uno smart contract, infatti, è un **sistema self-executing** che riceve istruzioni tramite il codice, elabora informazioni provenienti dall'esterno come input ed esegue delle azioni come output (ad esempio, il trasferimento di denaro tra i contraenti).

Tuttavia, alla base del funzionamento di tale meccanismo c'è la **fiducia delle parti che si vincolano** a uno smart contract, tale per cui esse di fatto rinunciano all'intervento di una terza parte (ad esempio, un giudice, un mediatore o un intermediario): ed è **qui che entrano in gioco i sistemi di blockchain**.

Sistemi di blockchain

In tal senso, infatti, vincolandosi a uno smart contract le parti non ne accettano solo le clausole, ma anche il sistema di funzionamento e la relativa automaticità, a fronte di un innegabile risparmio in termini di tempo e costi nelle fasi di esecuzione del contratto: ovviamente, ciò è possibile solo qualora si possa fare affidamento su **sistemi sicuri**, come appunto quelli di blockchain, **che garantiscono la tracciabilità delle operazioni** e rendono dunque superfluo l'intervento di un soggetto terzo, assicurando allo stesso modo i contraenti che l'esecuzione delle clausole contrattuali posta in essere corrisponda perfettamente agli esiti previsti dalla negoziazione stipulata dalle parti.

È interessante rilevare che l'**assenza di una terza parte** e di un intermediario - con l'eliminazione dei relativi costi - è proprio ciò che caratterizza anche i sistemi di blockchain.

Da un punto di vista tecnologico, il **blockchain** è definito come un **database replicato, distribuito e basato su una rete peer-to-peer**, che permette transazioni sicure senza l'intervento di controllo centralizzato: in questo contesto, il database replicato agisce come registro unico di monitoraggio di tutte le transazioni effettuate tra i partecipanti alla rete.

In particolare, mentre i primi sistemi blockchain erano stati sviluppati per la gestione delle c.d. valute virtuali (in particolare, di bitcoin), attualmente i nuovi sistemi sono concepiti per la **gestione di qualsiasi dato o contenuto digitale**. In effetti, i sistemi blockchain non si limitano necessariamente alle transazioni di valute virtuali, ma possono riferirsi alla gestione di qualsiasi elemento registrato nel database distribuito e replicato.

Per altro verso, come già accennato, sotto il profilo del funzionamento l'elemento che caratterizza i sistemi blockchain

è l'**assenza di un'autorità centrale gerarchica** che convalidi le operazioni registrate sul sistema, garantendo al contempo la massima trasparenza agli utenti in relazione a tutte le operazioni effettuate sui dati e sui contenuti presenti nel sistema.

Un sistema blockchain è quindi composto principalmente da **due ordini di elementi**: in primo luogo, dagli **utenti della rete** che possono svolgere operazioni sul sistema garantite da meccanismi di autenticazione, riferimento temporale e impronta informatica dei record; in secondo luogo, da una **rete di nodi peer-to-peer** utilizzata per registrare le operazioni e i relativi record e permettere agli utenti di verificare in modo trasparente e "orizzontale" il processo di convalida degli stessi. Nello specifico, infatti, ogni volta che un'operazione (o blocco di operazioni) viene convalidata, vengono trasmessi alla rete i relativi **record**. In particolare, a ogni blocco di operazioni è associato anche un record con il relativo riferimento univoco (ad esempio, l'hash[2]), nonché i riferimenti univoci al blocco di operazioni precedente: pertanto il blockchain costituisce fondamentalmente una catena di blocchi di operazioni a cui sono associati i relativi record.

Serve una regolamentazione

Questi **nuovi scenari**, quindi, delineano la concreta possibilità di combinare sistemi blockchain con smart contracts, eventualmente utilizzando anche le informazioni provenienti dai big data analytics. L'utilizzo concreto di tali sistemi combinati, infatti, è già da tempo studiato soprattutto in ambito bancario e finanziario (è sufficiente fare riferimento, a titolo esemplificativo, al contesto delle transazioni interbancarie), ma anche per ottimizzare il funzionamento di piattaforme di aste on line o di e-marketplace.

Si pensi proprio all'utilizzo dei sistemi blockchain in **ambito bancario o finanziario**: per quanto riguarda, ad esempio, la gestione di dati e informazioni, occorre considerare che ogni nodo del sistema ha facoltà di accesso all'intero database, dato che ogni punto deve poter controllare la validità delle transazioni e delle operazioni effettuate. Sotto il profilo strettamente giuridico, ciò comporta ovviamente che alcuni dati relativi ai clienti debbano essere criptati o anonimizzati, non solo qualora questi rappresentino dati personali riferiti a persone fisiche al fine di tutelare la privacy delle stesse, ma anche quando da essi siano ricavabili informazioni riservate riferite a persone giuridiche, la cui divulgazione possa recare danno alle stesse.

Accanto a tali aspetti, ovviamente, a seconda dell'ambito di riferimento, occorrerà regolamentare attentamente le **modalità di utilizzo** di sistemi blockchain o di smart contracts tra le parti (soprattutto qualora non ci si trovi in un contesto B2B), gli strumenti di autenticazione, le varie ipotesi di gestione dei dati e di accesso agli stessi, la titolarità e la riservatezza delle informazioni che vi transitano, la conservazione legale delle prove informatiche relative alle operazioni, nonché tutti gli ulteriori profili che dovessero venire in rilievo a seconda del contesto.

In definitiva, nell'ottica di risk management, i **potenziali vantaggi** derivanti dall'utilizzo di tali sistemi devono sicuramente portare a superare l'iniziale diffidenza verso gli stessi e le possibili criticità che questi possono comportare. Tuttavia, risulta indispensabile la **predisposizione di complesse regolamentazioni contrattuali** che non trascurino nessuno degli articolati profili tecnico-giuridici che li connotano.

AL DIG.EAT 2016 SI PARLERÀ DI

Smart contracts e sistemi di blockchain: quale regolamentazione?
Contratti IT, Business intelligence e Big data - Il risveglio della forza - Ore 16.15 – 17.45

[2] *Come precisato anche dalla definizione contenuta nell'Allegato I delle Regole tecniche del Dpcm 13 novembre 2014 (Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005), l'hash di un'evidenza informatica si ottiene applicando una funzione matematica che genera un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti. L'impronta dell'evidenza informatica, dunque, altro non è che la sequenza di simboli di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.*