Consiglio Nazionale del Notariato

AREA INFORMATICA

Studio n. 1/2017 DI

Il documento digitale nel tempo

(ES/MM/SC – novembre 2017)

Approvato dalla Commissione Informatica il 5 dicembre 2017
Approvato dal C.N.N. nella seduta del 22 e 23 febbraio 2018

Indice: 1. Introduzione generale: la specificità del documento informatico - 2. La firma digitale e le ragioni della sua validità limitata - 3. La marca temporale: funzione, caratteristiche ed oneri - 4. Il procedimento di conservazione a norma: cenni e funzione - 5. Altri sistemi di validazione temporale - 6. Il rapporto tra norme civilistiche e tecniche: la data certa del Pubblico Ufficiale e la data certa a' sensi dell'art. 2704 c.c. - 7. Il repertorio notarile quale sistema di etero datazione: limiti - 8. La verifica della firma digitale e funzione della "verifica alla data", limiti di corretto utilizzo - 9. Il documento informatico con firma scaduta.

Abstract:
I documenti cartacei sono un mezzo per trasmettere informazioni e conservarle. I documenti elettronici le trasmettono in maniera più efficiente ma le conservano in maniera meno efficiente, occorrendo a tal fine delle infrastrutture ad hoc.
In particolare, *l'affidabilit*à e l'autenticità di un documento informatico è legata esclusivamente alla sicurezza dei certificati di firma utilizzati per la sua sottoscrizione. Tale sicurezza, per essere mantenuta nel tempo, necessita di precisi processi tecnici di conservazione non surrogabili da procedure esterne.
In tale contesto la verifica della firma è processo centrale nella valutazione dell'affidabilità ed autenticità del documento e deve sempre essere effettuata con riferimento alla data concreta di utilizzo del documento. Effettuare tale verifica ad una specifica data anteriore (cosiddetta "verifica alla data") è processo da limitarsi rigorosamente ai soli ed esclusivi casi normativamente previsti ed in cui è possibile una etero datazione dell'intero documento e non solo dei suoi estremi con esclusione quindi di tutti i sistemi etero datazione parziale e non idonei a tale scopo.
Lo studio ripercorre la normativa vigente in materia, evidenziando le ragioni sottostanti alla previsione di cui *all'art.* 24 co. 4-bis del CAD che sancisce la perdita della sottoscrizione in relazione ad un documento la cui firma digitale sia scaduta, sospesa o revocata. Vengono quindi esaminate le soluzioni che la normativa (anche di natura tecnica) ha approntato per assicurare la validità dei documenti informatici nel tempo, con particolare riferimento alla conservazione a norma ed alla marcatura temporale. Vengono inoltre esaminati gli effetti giuridici della spedizione del documento a mezzo Posta Elettronica Certificata e della protocollazione informatica. Lo studio si sofferma infine su una analisi dei principali sistemi alternativi di datazione di un documento informatico (quali la registrazione o *l'iscrizione* a repertorio) evidenziandone i limiti.

1. Introduzione generale: la specificità del documento informatico

Il passare del tempo agisce in modo differente sul documento analogico e sul documento informatico[1] con conseguenze prima di tutto tecniche che si riverberano però direttamente sull'ambito giuridico.
Come noto, infatti, documento analogico e digitale, mentre sono identici dal punto di vista giuridico e sul significato che essi rappresentano, differiscono profondamente con riguardo alla loro intima natura e più che altro alla tecnica con cui sono composti.
Tale intima natura influisce direttamente sulle modalità e sui problemi di corretta conservazione di entrambi. Mentre nel caso del documento analogico la principale se non l'unica preoccupazione è quella di mantenere intatta la fisicità del documento, dei contrassegni ad esso apposti e del supporto su cui il documento è registrato al fine di consentirne la leggibilità, nel caso del documento digitale, accanto al problema di mantenere un valido supporto per lo stesso, vi è in aggiunta il problema di mantenere costantemente sicura e non alterabile la logica interna prettamente matematica con cui lo stesso è composto.
Tali diversità si riverberano in primo luogo anche sulla sottoscrizione e sulla firma che pur mantenendo identico significato giuridico, se sul documento analogico rappresenta pur sempre e solo un gesto umano che modifica il supporto, sul documento digitale - anche in caso di firma cosiddetta "grafometrica" - è in ultima analisi anch'essa esclusivamente un processo logico matematico.

Analizzando, per quel che qui ci occupa precipuamente, gli effetti e le modalità di conservazione della validità delle firme, una primissima osservazione e conseguenza viene all'occhio:
le firme digitali, a differenza delle firme autografe, perdono di validità nel tempo[2].
La ragione di tale singolare caratteristica - come accennato - prescinde da motivi puramente giuridici ed è strettamente legata alla particolare tecnologia su cui si basano tali firme che, con il passare del tempo e l'aumento di potenza di computazione dei computer, diventa sempre più debole.
La firma digitale infatti altro non è che una operazione particolarmente complessa di crittografia e di codifica del documento o meglio delle sue impronte a mezzo di chiavi di cifratura asimmetriche che consente - invertendo il procedimento crittografico di firma - di verificare a posteriori, ad un tempo, l'integrità e la provenienza di un documento. Tutto si basa però esclusivamente sulla complessità di tale procedimento matematico che tanto è più sicuro quanto più è difficile da replicare in maniera contraffatta.
Posto che tuttavia tale difficoltà risiede solo nella concreta complessità dei calcoli necessari ad alterare fraudolentemente tali processi crittografici è intuibile che tale complessità e quindi tale sicurezza vada via via scemando man mano che la potenza di calcolo degli elaboratori aumenta.
Man mano quindi che il tempo passa diventa sempre più agevole la creazione di documenti falsi[3].

Per dirla con una metafora, è come se l'inchiostro che compone il documento digitale o meglio la ceralacca che sigilla la busta in cui esso è contenuto - in assenza di azioni volte alla sua conservazione - vada via via a scomparire ed a sgretolarsi con il passare del tempo, rendendo sempre più agevole la sua contraffazione. E questo, si badi, a prescindere da chi sia l'autore

[1] Le definizioni di documento analogico e informatico sono contenute nell'art. 1 del Decreto Legislativo 82/2005 (Codice dell'Amministrazione Digitale) alle lettere *p) documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;* e *p-bis) documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.*

[2] R. ZAGAMI, Il fattore tempo: la marcatura temporale, Studio del CNN 6/2003: "*Mentre una sottoscrizione su carta, con il trascorrere del tempo, mantiene in via di principio lo stesso valore probatorio, diversamente una firma digitale, invece, è fin dall'inizio destinata a perdere sicurezza ed efficacia probatoria in breve tempo a seguito della sua necessaria scadenza (predeterminata) o per eventuale revoca o sospensione (anteriori alla scadenza)*".

[3] U. BECHINI, Contiene atto notarile: per la scadenza vedere sul tappo, Federnotizie, maggio 2001.

di tale documento, sia esso un privato cittadino, una Pubblica Amministrazione od un Pubblico Ufficiale.
La legge prevede quindi degli accorgimenti diretti ad evitare non tanto la scadenza della firma - che è inevitabile - quanto il suo effetto, cioè la perdita di validità della stessa e del documento a cui è apposta.

A tutto quanto sopra esposto deve aggiungersi che mentre per il documento analogico è impossibile immaginare la perdita od il furto della firma atteso che la stessa dipende esclusivamente da un intimo gesto umano, per il documento digitale tale eventualità non è affatto impossibile ed anzi deve essere disciplinata dal legislatore, considerato che la firma è, come detto, esclusivamente un processo matematico di crittografia, apposto attraverso un certificato solitamente residente su un supporto fisico (smart card o token) dotato di determinate credenziali e quindi passibile di smarrimento o furto.

2. La firma digitale e le ragioni della sua validità limitata. Analisi della normativa

Per tutto quanto sopra esposto, è intuitivo a questo punto comprendere le ragioni che hanno spinto il legislatore a dettare precise regole volte a disciplinare la validità della firma digitale nel tempo, le rigorose conseguenze in caso di sua scadenza e le modalità idonee a prolungare la sua validità.
Tali regole nella sostanza fondano la loro ratio nella stima grossolana dell'arco di tempo oltre il quale i processi matematici che salvaguardano l'autenticità del documento devono considerarsi non più sicuri, in quanto ormai facilmente aggirabili da sistemi di calcolo esponenzialmente sempre più potenti.

Il legislatore quindi dispone, in primo luogo, che la firma per essere valida deve essere apposta con un certificato sufficientemente sicuro e quindi aggiornato e valido. In secondo luogo, dispone che anche laddove il certificato fosse in origine adeguato e sicuro, e quindi il documento valido, esso possa corrompersi e perdere validità laddove il documento non sia adeguatamente conservato come infra meglio specificato, non differentemente da quanto farebbe un documento cartaceo i cui sigilli e contrassegni si rompano, si cancellino o risultino alterati, cosa che farebbe perdere una volta per sempre validità al documento, e - si badi - a prescindere da chi sia il soggetto firmatario, privato cittadino o pubblico ufficiale che sia.
Tutto questo ragionamento è tradotto nella normativa ad oggi in vigore attraverso una serie di norme all'interno del Codice dell'Amministrazione Digitale, nelle regole tecniche ed in altre norme collegate poste in coerente e serrata concatenazione.

Primo anello di tale catena normativa è innanzitutto l'art. 24 del CAD, rubricato "Firma digitale" che così dispone al comma 3:
"3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o *sospeso."*

Il certificato da utilizzarsi quindi deve ovviamente avere una chiave di lunghezza adeguata al momento in cui viene utilizzato ed essere pertanto in corso di validità, non revocato e non sospeso dal suo titolare.

Al successivo comma 4-bis si precisa ulteriormente:
"4-bis. L'apposizione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione"

Quello che accade quindi è che un documento a suo tempo validamente firmato, può degradare allo stato di documento non sottoscritto se il certificato utilizzato viene lasciato scadere o viene revocato o sospeso. Con una metafora, non differentemente da quello che accade ad una busta sigillata, la cui ceralacca con il tempo si sgretoli.

Invero, taluni ritengono che tale norma vada interpretata con esclusivo riferimento al momento genetico di formazione del documento. Si sosterrebbe, insomma, che sia sufficiente raggiungere la certezza che il certificato di firma "sia stato apposto" in un momento temporale nel quale il certificato di firma digitale non era ancora scaduto o revocato.

Una simile interpretazione, tuttavia, non può essere condivisa.
Del resto, al fine di interpretare correttamente la suddetta norma non è possibile prescindere dalle ragioni che stanno alla base della previsione normativa stessa: "Non si può *(…)* escludere che tra cinque anni violare una delle chiavi attualmente in uso divenga un compito relativamente semplice. Se così fosse, nel 2006 chiunque potrà produrre un documento provvisto di una perfetta ed ineccepibile firma digitale di Romolo Romani, datata 2001. E quindi i documenti sino a quel momento firmati con quella chiave cesseranno di essere affidabili, perché facilmente falsificabili."[4].

La norma, quindi, lungi dal prendere in considerazione il momento genetico del documento digitale, si riferisce al momento del suo successivo utilizzo e - quindi - della sua successiva verifica, statuendo il principio secondo cui, una volta scaduto, revocato o sospeso il certificato di firma, sussisterebbe una "presunzione legale di sopravvenuta inaffidabilità del documento" stesso.
E non potendo l'ordinamento accettare il rischio di imputare ad un soggetto un documento potenzialmente diverso da quello effettivamente sottoscritto, preferisce adottare la soluzione della "perdita sopravvenuta di imputabilità".

Lo confermano inoltre il quadro e la catena normativa. Infatti, proseguendo oltre, l'art. 62 delle regole tecniche in materia di firma digitale di cui al DPCM 22 febbraio 2013 a sua volta specifica che l'effetto di cui all'art. 24 comma 4 bis (perdita della sottoscrizione) non si verifica quando alla firma è associabile un riferimento temporale opponibile ai terzi che colloca l'esistenza del documento (e quindi la generazione della firma) in data anteriore a quella della scadenza o revoca. Quindi il documento pur se firmato con un certificato ormai scaduto può - come si vedrà, in determinate condizioni - mantenere validità, laddove sia comunque possibile datarlo ad un periodo all'interno della finestra di validità del certificato con il quale è firmato.

Parallelamente, l'art. 20 co. 3 del CAD specifica che la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.
Ultimo tassello del ragionamento è l'art. 41 del DPCM 22 febbraio 2013 citato ove sono elencati i riferimenti temporali opponibili ai terzi[5], tra cui ritroviamo l'apposizione di una marca temporale, il protocollo informatico, il riferimento temporale ottenuto con l'inserimento del documento in un sistema di conservazione a norma ad opera di un pubblico ufficiale, la spedizione del documento a mezzo PEC.

Per riassumere: i documenti informatici firmati digitalmente privi di alcuno dei riferimenti temporali previsti dalla normativa tecnica, una volta scaduto o revocato il certificato di firma

[4] U. BECHINI, Contiene atto notarile: per la scadenza vedere sul tappo, Federnotizie, maggio 2001

[5] Ovvero i sistemi di validazione temporale elettronica. Si ricorda che il DPCM è anteriore al Regolamento eIDAS, per cui non sempre le varie definizioni sono allineate.

digitale utilizzato per sottoscriverli, degradano da "originale" validamente sottoscritto a "riproduzione informatica di fatti o cose"[6], con l'efficacia di cui all'art. 2712 c.c. Infatti, una volta scaduto il certificato di firma digitale, è vero che il documento informatico in quanto tale è giuridicamente evaporato[7], ma rimane il fatto storico documentato[8].

3. La marca temporale: funzione, caratteristiche ed oneri

Prima di introdurre il concetto di marca temporale è necessario accennare ad un'importante precisazione da essere poi in seguito meglio dettagliata che chiarisce il motivo per cui per il documento informatico non sono sufficienti le normali regole civilistiche di cui all'art. 2704 c.c. sulla datazione ed etero datazione del documento ma sono necessarie anche regole tecniche precise.

Come accennato sopra, nel caso di documento cartaceo, la firma è un'azione umana che modifica fisicamente il supporto su cui il documento è redatto, rimanendo, una volta apposta, immodificabile. Datare quindi la firma, o comunque la conclusione del documento o la sua protocollazione o messa a repertorio, o ancora disporre di un qualsiasi elemento di etero datazione significa automaticamente datare anche il documento nella sua interezza.

Generalizzando, è sufficiente datare "un pezzo" del documento - che sia un "pezzo" fisico o logico - (ad esempio con un timbro a margine o in calce o sapere che uno dei firmatari è divenuto nell'impossibilità di sottoscrivere successivamente alla apposizione della firma) per datare l'intero documento, perché il supporto fisico su cui il documento inerisce è esso stesso garante di conservazione ed inalterabilità.

Per il documento informatico invece questo ragionamento non vale, perché non abbiamo il supporto fisico del documento a fare da garante di immodificabilità. E anche la firma del documento informatico - come accennato - è un'azione profondamente diversa, che rimane sempre una mera operazione crittografica e matematica che non fa che aggiungere altri numeri ed altri bit ai numeri ed ai bit del documento ponendoli in relazione logica con essi.

Il documento informatico quindi nella sostanza, privo del supporto materiale che caratterizza il documento analogico, è costretto ad essere supporto di se stesso, e ad essere autonomo ed auto consistente.
E' la stessa sua logica interna - ed essa sola - ad essere garanzia di autenticità e di immodificabilità, logica che se corrotta o ormai desueta e quindi scaduta compromette tutto il documento nella sua interezza.

Per tutto quanto esposto, la datazione del documento informatico quindi non può limitarsi ad un elemento che sia esterno o parziale, come per il documento cartaceo e come, ad esempio, la sua messa a repertorio ma deve investire ogni singolo bit ed ogni singolo elemento del

---

[6] In pratica la stessa differenza che, nel mondo cartaceo, abbiamo tra un originale ed una semplice fotocopia.

[7] Il fatto che la firma digitale "scada" è una caratteristica che può destare stupore o financo scandalizzare il giurista alle prime armi con il diritto dell'informatica ma a ben vedere è un fenomeno che l'umanità ha, almeno concettualmente, da qualche secolo sotto gli occhi solo in forma leggermente diversa. Basti pensare alle normali banconote. Anch'esse sono progettate e realizzate con tutta una serie di accorgimenti tecnici quali filigrane, micro stampe, rilievi, colori e fantasie complesse, al fine di essere sostanzialmente impossibili o comunque molto difficili da replicare perfettamente in modo fraudolento. Tale complessità tuttavia decresce esponenzialmente con il passare del tempo al progredire della tecnica e della tecnologia e proprio per ovviare a tale perdita di sicurezza gli stati di tutto il modo periodicamente "fanno scadere" e rinnovano le banconote esistenti quando ritengono che le stesse non siano più sicure, ritirandole dalla circolazione ed offrendo di sostituirle con altrettante banconote nuove. Chi si attardasse nella loro sostituzione e le lasciasse scadere definitivamente si troverebbe con un pugno di carta straccia, non differentemente da quello che accade con il documento informatico con firma scaduta.

[8] U. BECHINI, Contiene atto notarile: per la scadenza vedere sul tappo, Federnotizie, maggio 2001.

documento, perché altrimenti lo stesso - privo di supporto - è comunque esposto a modifiche e contraffazioni. Poco infatti serve sapere che il documento (o meglio "un certo documento") genericamente descritto per meri estremi esisteva ad una tale data, perché se nel frattempo il documento perde l'incorruttibilità della propria logica interna a causa dell'invecchiamento degli algoritmi che lo costituiscono - ad esempio per scadenza della firma - sarà esposto a qualsiasi tipo di falsificazioni ed alterazioni e nella sostanza anche dal punto di vista civilistico degraderà da documento autentico a semplice riproduzione o "fotocopia" del vecchio documento. Ed una volta degradato a tale stato giuridico pressoché inutile sarà qualsiasi tentativo di etero datazione come inutile sarebbe cercare di riportare allo stato di documento autentico una semplice fotocopia cartacea basandosi solo su elementi di etero datazione e senza ri-collazionare interamente tutto il documento con l'intervento di un Pubblico Ufficiale.[9]

Ecco quindi che il sistema principale previsto dal legislatore per datare il documento informatico - vale a dire la marca temporale[10] - opera con una logica completamente differente dai sistemi di datazione del documento cartaceo e quindi è anch'essa se analizzata nei suoi elementi di base null'altro se non un'operazione di logica matematica che "investe" ogni singolo elemento ed ogni singolo bit del documento garantendone l'inalterabilità. Come la migliore dottrina ha rilevato la datazione del documento informatico non può che riguardare il documento nella sua interezza e mai può essere parziale.[11]

Come accennato e come noto la marca temporale altro non è che una particolare operazione di crittografia asimmetrica analoga a quella che avviene in caso di firma digitale, apposta da una Autorità di Marcatura Temporale o Time Stamping Authority, che funge da terzo fidato, e che contiene al proprio interno oltre ai dati della firma anche i dati di ora e giorno di apposizione[12].
Funzione della marca è assicurare che il documento o meglio "quel preciso documento" in tutti i suoi bit e nella sua interezza fosse esistente ad una determinata data, né più ne meno di un normale "timbro postale". La marca temporale tuttavia come è facile cogliere rappresenta un sistema di datazione non assoluto, ma relativo o parziale, limitandosi ad essere una data certa "entro" cui quel determinato documento è considerato esistente, come diversi già ne esistono nel nostro ordinamento e come potrebbe essere ad esempio la registrazione dell'atto e che differisce pertanto dalla data certa "assoluta" che è conferita dalla autentica o dal ricevimento da parte del pubblico ufficiale.

Anche la marca temporale tuttavia non è un processo definitivo ma posto che anch'essa fa risiedere la sua sicurezza sulla complessità oggettiva di una sua falsificazione anch'essa è soggetta a scadenza, seppur più remota. Non è quindi la marca temporale ad assicurare la

---

[9] Tale ricostruzione appare corretta anche dal punto di vista della diplomatica vale a dire come è noto della scienza che si occupa di studiare l'autenticità dei documenti e la loro corretta archiviazione. Per tale disciplina concetto fondamentale è quello della catena ininterrotta di custodia, cosiddetta "chain of custody" e di custodia intatta ovvero di "unbroken custody". Fin tanto che un determinato documento rimane nella disponibilità fisica del suo autore o dell'ente che lo ha prodotto o di terzi che offrano uguale affidabilità può considerarsi autentico. Ugualmente fin tanto che tale documento rimane protetto dai sigilli che ne garantiscono l'autenticità esso può intendersi autentico. La rottura della catena di custodia ha effetto radicale sulla validità del documento a fini archivistici e non può essere recuperata se non ripartendo dalla radice della catena a nulla valendo eventuali sistemi parziali di ricostruzione del documento.
Anche dal punto di vista archivistico e documentale quindi il materiale documentario uscito dalla unbroken custody dell'ente produttore e dei suoi legittimi successori o che risulti corrotto cessa di avere il carattere di «autenticità» e, per conseguenza, venendo ad esso meno uno dei requisiti archivistici essenziali, cessa radicalmente di essere considerato parte dell'archivio.

[10] La marca temporale è la validazione temporale elettronica disciplinata dal Titolo IV del DPCM 22 febbraio 2013 (*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*). La nozione di validazione temporale elettronica è invece contenuta nel Regolamento eIDAS (Regolamento UE n. 910/2014) nel quale è definita come "*dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento*".

[11] R. ZAGAMI, Firma digitale e sicurezza giuridica, CEDAM, 2001

[12] A tal proposito, il regolamento eIDAS parla di "*validazione temporale elettronica qualificata*".

conservazione definitiva e permanente del documento, ma piuttosto un corretto processo di conservazione a norma, più innanzi dettagliato.

A questo punto ci si può chiedere a chi spetti l'apposizione della marca temporale.
A tal proposito, posto che l'apposizione della marca è una azione volta a prolungare la conservazione del documento può qualificarsi la stessa correttamente come "onere" - vale a dire come una azione richiesta, al fine di ottenere un determinato risultato giuridico - e può forse dirsi che tale onere segua di pari passo l'onere di conservazione, e quindi che chi debba o abbia interesse a conservare il documento dovrà parallelamente o avrà parimenti interesse ad apporre la marca temporale al fine di assicurare il prolungamento di validità del documento per il tempo di suo interesse, nell'attesa - se del caso - di assoggettarlo ad un definitivo processo di conservazione a norma.[13]

In ambito notarile pertanto il notaio potrà validamente emettere od inviare documenti firmati digitalmente senza essere onerato di apporre marche temporali agli stessi. Saranno i soggetti interessati se del caso ad eseguire la relativa operazione per il tempo ritenuto necessario.
Un piccolo temperamento tuttavia a quanto appena detto può forse effettuarsi laddove il notaio si accinga a firmare documenti con certificati di firma che siano prossimi alla scadenza. In tal caso, in un'ottica di buona pratica, può forse considerarsi comportamento attento e scrupoloso quello di sottoporre il documento a marcatura temporale al fine di non mettere in eccessiva difficoltà il destinatario, soprattutto alla luce di quanto si dirà più avanti.

4. Il procedimento di conservazione a norma: cenni e funzione

Le funzioni fondamentali dei sistemi di conservazione a norma sono molteplici. Esse sono elencate all'art. 44 del CAD e poi ribadite all'art. 3 delle regole tecniche in materia di conservazione (DPCM 3 dicembre 2013). Proprio in tale ultima norma è specificato che il sistema garantisce "le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità".

Limitandosi agli aspetti che qui interessano[14] e soffermandosi sulla prima di tali caratteristiche, è evidente come il mantenimento dell'autenticità non possa che passare per il mantenimento della validità della firma apposta ai documenti conservati.
Poiché, come abbiamo visto, anche la marca temporale di un documento informatico non è un processo definitivo, essendo anch'essa soggetta a scadenza, seppur più remota, il mantenimento dell'autenticità di un documento non può prescindere dal deposito del medesimo all'interno di un "ambiente" a ciò deputato per legge.

---

[13] Merita qui di essere ricordata la questione della validità degli attestati di prestazione energetica (APE) di alcune regioni italiane (Piemonte e Lombardia, *in primis*) che, formati in originale digitale, sono poi depositati presso i sistemi informativi regionali, che però non sono sistemi di conservazione a norma. Sulle conseguenze della inevitabile perdita della sottoscrizione con la scadenza del relativo certificato di firma si è pronunciato anche l'Ufficio Studi del Consiglio Nazionale del Notariato con la risposta a quesito n. 7-2014/DI dell'11 marzo 2014 pubblicato su CNN Notizie del 18 marzo 2014, concludendo che comunque la mancanza di sottoscrizione non costituisce un ostacolo all'utilizzo del documento, considerato che il legislatore prevede la possibilità di allegare una semplice copia dell'APE e non necessariamente l'originale.
Successivamente, in materia è intervenuto il Ministero dell'Economia e delle Finanze, che con Decreto del 26 giugno 2015 ha, tra l'altro, stabilito che "*Nel caso in cui l'APE sia sottoscritto con firma digitale e venga depositato su catasti o registri telematici appositamente creati dalle Pubbliche Amministrazioni o da loro enti o società in house non è necessaria la marcatura temporale ai fini del riconoscimento del suo valore legale per tutti gli usi previsti dalla legge. L'APE firmato digitalmente resta valido..., a prescindere dall'eventuale successiva cessazione del contratto di autorizzazione del soggetto certificatore alla firma digitale*", con buona pace dei principi in materia di gerarchia delle fonti. Sul punto, più diffusamente, si veda A. Lisi, G. Penzo Doria, E. Stucchi, *Documenti digitali - Se le norme del digitale sono un pasticcio: il caso dell'attestato di prestazione energetica*, su http://www.forumpa.it/pa-digitale/la-validita-atemporale-dellattestato-di-prestazione-energetica-da-winnie-the-pooh-allape-maia.

[14] La conservazione a norma è argomento vasto e complesso la cui trattazione va ben al di là del presente studio.

A tale ultimo fine, l'art. 9 delle regole tecniche statuisce che il processo di conservazione prevede, tra l'altro, la generazione di un rapporto di versamento "contenente un riferimento temporale". E' evidente quindi come, per ogni documento inserito nel sistema di conservazione a norma, sia rinvenibile una data e ora alla quale collocare l'esistenza del documento stesso.

Si può quindi prevedere che, con il trascorrere del tempo e la conseguente scadenza dei certificati di firma associati ai documenti inseriti, il sistema di conservazione, in fase di esibizione, produrrà copie piuttosto che rilasciare un duplicato dell'originale.
Quest'ultimo infatti non avrà più alcun valore se non accompagnato da una certificazione del responsabile della conservazione che ne attesti la conformità, autenticità ed integrità rispetto al momento di conservazione stesso di cui al riferimento temporale ad esso associato.

Con riferimento, in particolare, agli atti notarili conservati a raccolta, si può concludere che sarà cura del notaio, responsabile della conservazione dei suoi atti, rilasciare copia autentica, sottoscritta di volta in volta con il certificato di firma valido a quel momento.

Diverso discorso va fatto per gli atti rilasciati, i quali, se non conservati in un sistema rispondente ai requisiti di cui al DPCM 3 dicembre 2013, con relativa certificazione del responsabile della conservazione, perderanno definitivamente l'elemento di autenticità.

5. Altri sistemi di validazione temporale

Come sopra chiarito, l'art. 41 delle regole tecniche in materia di firma digitale (DPCM 22 febbraio 2013) elenca i riferimenti temporali opponibili ai terzi. Oltre alla marca temporale e alla conservazione a norma, descritte nei paragrafi che precedono, meritano qui un cenno il protocollo informatico e la posta elettronica certificata.

Il protocollo è una delle fasi del flusso documentale ricevuto e spedito dalla pubblica amministrazione. In particolare, ad ogni documento viene assegnato un numero progressivo del registro di protocollo, per poi essere classificato, fascicolato e conservato.
Come stabilito dal DPCM 3 dicembre 2013 in materia di protocollo informatico, a partire dall'11 ottobre 2015 le Pubbliche Amministrazioni sono tenute a inviare in conservazione il registro giornaliero di protocollo entro la giornata lavorativa successiva.

Il registro giornaliero di protocollo deve ricomprendere le informazioni minime richieste dall'art. 53, co. 1, del DPR 445/2000 e dalla Circolare AgID n. 60 del 23 gennaio 2013, tra cui "la data di registrazione di protocollo... registrata in forma non modificabile" e "*l'impronta* del documento informatico, se trasmesso per via telematica". Il protocollo informatico, pertanto, attestante numero e data, è idoneo, per le sue caratteristiche tecniche[15], ad attribuire al documento un riferimento temporale al quale far risalire la sua esistenza, consentendo di procedere alla verifica della firma alla data dello stesso.

Quanto alla PEC, la sua idoneità a costituire riferimento temporale opponibile ai terzi deriva dal particolare meccanismo di funzionamento. Infatti, il gestore di PEC invia al mittente una ricevuta di accettazione con le seguenti informazioni: data e ora dell'invio, mittente, destinatario, oggetto e identificativo del messaggio.
Il messaggio viene quindi "imbustato" in un altro messaggio, chiamato "busta di trasporto" che il gestore provvede a firmare digitalmente. Questa operazione consente di certificare ufficialmente l'invio e la consegna del messaggio nonché la data e l'ora ad essi associate.

[15] Come precisato, il registro di protocollo contiene l'impronta del documento e pertanto è connesso allo stesso in maniera tale da poter sempre provare se il documento protocollato sia stato successivamente alterato.

Pertanto, ad un documento firmato digitalmente che sia incluso quale allegato in una PEC è attribuita come data certa quella attestata dal gestore e da quest'ultimo firmata digitalmente.

E' possibile trovare conferma di quanto finora esposto anche nell'art. 43 del 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 (regolamento noto con l'acronimo di eIDAS)[16] pubblicato 28 agosto 2014 nella Gazzetta Ufficiale dell'Unione Europea (EU Official Journal L 257).
Tale ultimo articolo, infatti, prevede espressamente che "I dati inviati e ricevuti mediante servizio elettronico di recapito certificato qualificato godono della presunzione di integrità dei dati, *dell'invio* di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e *dell'ora dell'invio* e della ricezione indicate dal servizio elettronico di recapito certificato qualificato."

6. Il rapporto tra norme civilistiche e tecniche: la data certa del Pubblico Ufficiale e la data certa ai sensi **dell'art.** 2704 c.c.

Un documento ha data certa quando e' possibile provare erga omnes la sua esistenza in un certo arco temporale o comunque anteriormente ad un dato evento.

Le norme civilistiche che regolano la prova documentale sono dettate, com'è noto, principalmente agli articoli 2699 e seguenti c.c..

In tutti i casi di intervento di un pubblico ufficiale (atto pubblico, scrittura privata autenticata) e' proprio l'intervento di quest'ultimo a rendere la data certa. All'intervento del notaio è associata, di solito, l'iscrizione dell'atto (o meglio dei suoi elementi essenziali) nel repertorio con attribuzione di un numero progressivo associato ad una certa data.
Dal punto di vista civilistico, tale conclusione è sicuramente valida anche per i documenti informatici. Non altrettanto può dirsi dal punto di vista tecnico-informatico, cioè della sua idoneità ad evitare l'effetto di cui all'art. 24 co. 4-bis del CAD: l'iscrizione di un atto nel repertorio notarile, come infatti sarà chiarito più avanti, non può integrare quelle funzioni che la legge attribuisce alla validazione temporale, cioè evitare che le vicende successive del certificato utilizzato per firmare un certo documento (scadenza o revoca) ne inficino la validita'.

Il regolamento eIDAS (in vigore dal 1 luglio 2016) definisce "validazione temporale elettronica" come dati in forma elettronica che collegano altri dati in forma elettronica ad una particolare ora e data, così da provare che questi ultimi esistevano in quel momento.
Inoltre, come già ricordato sopra, l'art. 20 co. 3 del CAD specifica che la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

Volendo quindi chiarire il rapporto tra i due fenomeni, potremmo dire che la data apposta dal pubblico ufficiale costituisce data certa ai fini degli effetti civilistici del documento ed e' contestuale alla formazione del documento stesso, sempre che il suo contenuto risulti "sicuro" da un punto di vista informatico, cioè sempre che la verifica sulla firma digitale del notaio sia positiva.
La validazione temporale costituisce data certa in quanto destinata a dimostrare che un certo documento e' stato firmato prima della scadenza del certificato di firma utilizzato e puo' essere

[16] Il regolamento eIDAS abroga la direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche.

apposta anche molto tempo dopo la formazione del documento stesso, purché prima della scadenza del certificato[17]. Essa quindi non influenza in alcun modo la determinazione della data certa a fini civilistici, che rimane regolata dalle norme sue proprie.

Riassumendo, la data indicata in un documento sottoscritto dal notaio costituisce data certa ai fini degli effetti civilistici del documento ed è contestuale alla formazione del documento stesso, in quanto è l'ordinamento stesso ad attribuire tale valenza alla dichiarazione del pubblico ufficiale.
Ciò, pertanto, sarà sufficiente a mantenere la validità del documento anche nel caso in cui esso sia stato sottoscritto dalle parti mediante una firma digitale che risulti successivamente scaduta o revocata al momento della verifica del documento.
In altre parole, la scadenza o revoca del certificato di firma utilizzato da una delle parti in un atto pubblico o in una scrittura privata autenticata intervenute dopo la formazione del documento stesso non comporta l'applicazione dei principi di cui al co. 4 bis dell'art. 24 del CAD (perdita della sottoscrizione) in quanto la validità della sottoscrizione è "retta" dalla datazione certa attribuita dal pubblico ufficiale che colloca l'esistenza del documento (e quindi la generazione della firma) in data anteriore a quella della scadenza o revoca.

Ma poiché la datazione certa si regge sui poteri attribuiti dall'ordinamento al pubblico ufficiale, il predetto ragionamento potrà applicarsi se, ed in quanto, la sottoscrizione digitale del notaio (o del pubblico ufficiale) non sia essa stessa scaduta, sospesa o revocata.
In tal caso, infatti, la sottoscrizione stessa del pubblico ufficiale si avrebbe come non apposta, ed il documento (privo della firma del notaio) perderebbe la qualifica stessa di atto pubblico o di scrittura privata autenticata, e con essa ogni relativa efficacia probatoria.

In tale prospettiva, pertanto, appare necessario analizzare se vi siano altri strumenti di etero datazione di un documento informatico che consentano di assicurarne la validità nel tempo, in previsione del fatto che, al momento della sua verifica, anche (o solo) la firma digitale del notaio o del pubblico ufficiale risulti scaduta, sospesa o revocata.

Si potrebbe, ad esempio, ricorrere alla registrazione dell'atto quale sistema di etero datazione certa ai sensi dell'art. 2704 c.c., utilizzando l'efficacia probatoria offerta dall'intervenuta registrazione dell'atto per sostenere l'esistenza del documento a tale data.
Invero, tale strumento di datazione (soprattutto oggi che anche la registrazione avviene con modalità informatiche) attribuisce data certa non tanto al documento "originale", quanto piuttosto alla relativa copia o duplicato che viene trasmesso all'Agenzia delle Entrate.
La registrazione, infatti, non impedisce affatto che l'esemplare del documento informatico che invece rimane alle parti e gira tra esse ed i terzi venga successivamente manomesso o alterato, la qual cosa - peraltro - può avvenire anche nel mondo degli atti analogici (o cartacei che dir si voglia).
La differenza, com'è già stato ricordato, è che una alterazione di un documento analogico è visibile all'esame umano, mentre l'alterazione di un documento informatico non lo è.

Di conseguenza, un documento notarile informatico che sia stato rilasciato in "originale" e la cui sottoscrizione notarile digitale sia successivamente scaduta, sospesa o revocata, perderà comunque la propria validità giuridica ancorché esso sia stato sottoposto a registrazione in data anteriore al verificarsi di quanto previsto dal co. 4 bis dell'art. 24 del CAD (perdita della sottoscrizione).
Se, infatti, è possibile sostenere che la copia conservata presso i registri dell'Agenzia delle Entrate non perde l'efficacia che ne è propria, ciò non consente anche di sostenere che la "presenza" di tale copia sia di per sé idonea a prorogare nel tempo anche la validità

[17] S. CHIBBARO, Codice dell'Amministrazione Digitale, firme elettroniche e attività notarile, Studio CNN 2-2006/IG

dell'esemplare originale che, invece, vive di una "vita propria" e quindi può essere sempre autonomamente soggetto ad interventi di alterazione, manomissione o distruzione ad opera di terzi. In altre parole il documento informatico "scaduto" ma registrato potrebbe acquisire valenza solo previo raffronto con la copia depositata presso l'Agenzia delle Entrate. Ciò tuttavia, in primo luogo, esclude comunque che il documento scaduto possa avere una autonoma rilevanza, ed in secondo luogo evidenzia come sia comunque necessaria una sorta di attività comparativa e ricostruttiva che il nostro ordinamento riserva probabilmente solo all'autorità giudiziaria[18].

Infine, l'art. 2704 fa salvo "ogni altro fatto che stabilisca in modo egualmente certo *l'anteriorità* della formazione del documento".
Dati i principi qui enunciati, è evidente come tale "altro fatto" debba essere comunque riferibile all'intero documento, come peraltro più avanti sarà meglio chiarito.

7. Il repertorio notarile quale sistema di etero datazione: limiti

Un'ulteriore possibile soluzione per tentare di estendere la validità nel tempo di documenti notarili informatici nei quali la firma digitale del notaio rogante sia scaduta, sospesa o revocata, consisterebbe, secondo taluni, nel ricorso al repertorio notarile.
Com'è noto, infatti, i repertori sono i registri nei quali il notaio deve annotare, entro il giorno successivo, gli atti dal medesimo ricevuti o autenticati, con l'indicazione dei loro estremi secondo le modalità ed i criteri stabiliti dalla legge.
La natura giuridica (e di conseguenza l'efficacia probatoria) di tali repertori è stata, nel corso del tempo, assai dibattuta in dottrina e giurisprudenza.

Ripercorrendo brevemente le tre distinte impostazioni, possiamo ricordare una prima tesi secondo cui i repertori notarili non avrebbero natura pubblicistica e non avrebbero pertanto l'attitudine a fare piena prova fino a querela di falso[19]. All'estremo opposto, invece, si colloca l'ulteriore tesi secondo cui i repertori notarili avrebbero una natura pubblicistica tale da conferire piena prova ad ogni loro annotazione[20]. Nel mezzo, invece, si colloca quella tesi secondo cui dovrebbe distinguersi tra le annotazioni aventi una propria autonoma rilevanza e precisi effetti giuridici da quelle che tali caratteristiche non hanno. Secondo tale ultima tesi, infatti, l'efficacia probatoria delle iscrizioni repertoriali sarebbe circoscritta unicamente alla data di ricevimento dell'atto o di autenticazione ed ai dati identificativi delle parti[21].

Pur nella diversità di gradazioni, quindi, dottrina e giurisprudenza prevalenti sono concordi nel ritenere che i repertori notarili abbiano natura pubblicistica e - pertanto - facciano piena prova, quantomeno in relazione alla data dell'atto.

---

[18] Invero il caso in esame (di atto notarile informatico con firma digitale scaduta, ma preventivamente sottoposto a registrazione) potrebbe ben essere assimilato all'ipotesi di intervenuta perdita o distruzione di un atto. Potrebbe allora invocarsi in via analogica il disposto dell'art. 62-quater L.N. il quale prevede che gli atti di cui il notaio ha l'obbligo di conservazione e che siano persi possano essere ricostruiti - previo ricorso al Presidente del Tribunale competente - utilizzando "*anche altre registrazioni informatiche conservate presso lo stesso notaio che ha formato l'atto ovvero presso pubblici registri ovvero, in mancanza, una copia autentica dello stesso da chiunque posseduta*". Si tratterà comunque di un'operazione ricostruttiva che non "salva" il documento digitale scaduto, ma genera un nuovo documento la cui validità giuridica deriva non più dall'originale, ma dalla copia di esso depositata presso altri pubblici registri.

[19] Appello ROMA, 25 febbraio 1963; conforme in dottrina FALZONE-ALIBRANDI, 1973-1977.

[20] In applicazione di tale principio il Tribunale di TREVISO, con sentenza 12 maggio 1941, stabilì che poteva procedersi alla cancellazione di un'ipoteca il cui titolo era stato smarrito, sulla base di una attestazione da parte del notaio autenticante tratta dal repertorio.

[21] In tal senso Tribunale VERONA 6 marzo-22 maggio 1954, Cassazione Civile 26 luglio 1962 n. 2121, Cassazione Penale 30 gennaio 1979 n. 3362; conforme in dottrina PROTETTI'-DI ZENZO.

Ciò potrebbe allora bastare per fare di essi un mezzo idoneo di etero datazione anche di un documento informatico che, al momento della verifica, presenti la firma scaduta, sospesa o revocata del notaio (o del pubblico ufficiale).

In verità il ragionamento prova troppo.

Anche esulando, per un momento, dall'ambito informatico, giova infatti osservare che il repertorio non può essere utilizzato per attribuire validità ad un atto che, di per sé, non l'avrebbe.
In altre parole, il repertorio non vale a sanare eventuali mancanze proprie del documento in esso annotato.
Se, infatti, immaginassimo di avere di fronte un atto pubblico redatto su carta, ma privo della sottoscrizione del notaio, nessuno penserebbe di poter attribuire ad esso efficacia solo ed unicamente sulla base del fatto che esso risulta annotato nel repertorio degli atti tra vivi di quello stesso notaio.

Ebbene, il ragionamento con il documento informatico potrebbe essere identico: poichè - come abbiamo visto - la scadenza, sospensione o revoca della firma digitale del notaio equivale a mancanza della sottoscrizione, a nulla varrebbe il riferimento temporale offerto dal repertorio in quanto esso, comunque, si riferirebbe ad un documento nel quale la firma del notaio è stata "cancellata per legge".

Invero, richiamando l'interpretazione, sopra riportata, che vorrebbe che il più volte citato art. 4-bis[22] vada interpretata con esclusivo riferimento al momento genetico di formazione del documento, si sosterrebbe che sia sufficiente raggiungere la certezza che il certificato di firma "sia stato apposto" in un momento temporale nel quale il certificato di firma digitale non era ancora scaduto o revocato. Ed in questo, le risultanze del repertorio potrebbero costituire lo strumento idoneo.

Ma, se così fosse, una volta apposta una marcatura temporale ad un documento informatico, essa sarebbe idonea ad estenderne indefinitamente la validità nel tempo.
Ed invece, come abbiamo già visto, così non è.

Del resto, è esattamente questo il motivo per cui, nel mondo digitale, anche altri strumenti di datazione certa che vigono nel mondo analogico non possono essere considerati applicabili.
Si pensi, ad esempio, alla sopravvenuta morte del sottoscrittore che - nel mondo analogico - attribuisce data certa ad un documento cartaceo sottoscritto, mentre altrettanto non può dirsi per il documento informatico per il semplice motivo che, una volta violato il procedimento matematico posto alla base di una firma digitale, essa potrà essere apposta da terzi anche dopo la morte del soggetto che ne era titolare[23].

8. La verifica della firma digitale e funzione della **"verifica** alla **data",** limiti di corretto utilizzo

Quanto finora esposto deve allora invitare l'operatore alla prudenza allorquando egli si imbatta in un documento sottoscritto con certificato di firma digitale che - al momento della verifica - risulti essere scaduto, sospeso o revocato.

---

[22] *L'apposizione a un documento informatico di una firma digitale (...) basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione*

[23] R. ZAGAMI, Il fattore tempo: la marcatura temporale, Studio del CNN 6/2003

La tentazione, infatti, è quella di utilizzare una particolare funzione presente in quasi tutti i software di verifica che consiste nella "verifica ad una certa data", cioè nella possibilità di chiedere al sistema di effettuare una verifica non alla data odierna, ma ad una diversa ed antecedente data; come se una macchina del tempo consentisse di riportare indietro l'orologio ad una data precedente.

E' evidente che qualunque documento informatico con firma digitale scaduta verrebbe considerato "valido" se riportassimo indietro l'orologio del tempo ad una data nel quale il certificato era formalmente ancora vigente.

Ma a quale data è lecito portare indietro le lancette dell'orologio?

Chi ha seguito il ragionamento fin qui espresso non avrà difficoltà a rispondere che sarà lecito fare riferimento solo ad una data nella quale vi è la certezza che l'intero documento nel suo complesso (e quindi non solo la firma digitale) era esistente in quella precisa composizione (rectius in quella precisa sequenza binaria).

Un esempio pratico chiarirà maggiormente il concetto.
Supponiamo che il notaio Romolo Romani abbia ricevuto dal collega Tizio Tizi una copia digitale di procura cartacea datata 13 maggio 2017, sottoscritta dal notaio Tizio Tizi con firma digitale scadente il 10 novembre 2017, e che tale procura sia stata trasmessa dal notaio Tizio Tizi al notaio Romolo Romani a mezzo PEC in data 8 novembre 2017 (quindi due giorni prima della scadenza).
La verifica del file alla data odierna darà, ovviamente, esito negativo, a causa della intervenuta scadenza del certificato di firma.
Il notaio Romolo Romani dovrà allora chiedere al collega il rilascio di una nuova copia della procura? Oppure il file potrà essere legittimamente verificato ad una diversa data, anteriore alla data di scadenza del certificato di firma?

Per quanto detto prima, la verifica non potrà essere effettuata alla data del 13 maggio 2017 (data di creazione del documento), e ciò indipendentemente da quanto abbiamo sopra precisato con riguardo alla datazione derivante dall'annotazione a repertorio. Infatti, nemmeno la circostanza che il file in questione "appaia" essere stato creato il 13 maggio 2017 può avere una qualche rilevanza giuridica, e ciò nemmeno allorquando sia il software di verifica stesso ad indicare quella come data presunta di apposizione della firma.
Tale data, infatti, è solo quella che proviene dal software di apposizione della firma, che a sua volta non è un riferimento temporale certo, ma unicamente la data alla quale era impostato il computer utilizzato per l'operazione di firma.
Essendo però la data di un computer "un dato sotto il totale controllo dell'utilizzatore, facilmente alterabile da chiunque, è evidente come tale riferimento temporale sia assolutamente privo di alcun valore giuridico"[24].

Invece la verifica potrà essere legittimamente effettuata alla data del giorno 8 novembre 2017, data di trasmissione della PEC, in virtù di quanto sopra esposto in merito.
Non va infatti dimenticato che - in materia di Posta Elettronica Certificata - ai sensi dell'art. 6, comma 4, del DPR 11 febbraio 2005 n. 68 "La ricevuta di avvenuta consegna puo' contenere anche la copia completa del messaggio di posta elettronica certificata consegnato secondo quanto specificato dalle regole tecniche di cui all'articolo 17.".
Il che significa che la PEC rappresenta uno strumento idoneo ad attestare - con piena opponibilità erga omnes - che nella data di spedizione del messaggio un documento

[24] S. CHIBBARO, Codice dell'Amministrazione Digitale, firme elettroniche e attività notarile, Studio CNN 2-2006/IG

informatico ad essa allegato era esistente “in quella precisa forma ed in quella precisa consistenza binaria”.
In altre parole, è la stessa PEC ad assicurare che un preciso documento contenuto in un messaggio aveva quella precisa sequenza binaria in quella precisa data.
Il tutto con piena opponibilità ai terzi.
Ne consegue che il Notaio Romolo Romani, anche in data odierna (e quindi a certificato di firma scaduto) potrà comunque ancora utilizzare quel preciso file allegato alla PEC del giorno 8 novembre 2017 e verificarlo esattamente “alla data dell’8 novembre 2017”, ottenendo in questo caso una validazione retroattiva del documento stesso, ma valida ed opponibile ancor oggi.

9. Il documento informatico con firma scaduta

In conclusione, è possibile affermare che l’intervenuta scadenza della firma digitale del notaio, apposta ad un documento notarile informatico, determina ciò che potremmo definire una presunzione legale che quel documento possa essere (stato) alterato, con la conseguenza che di detto documento viene sancita la totale perdita di rilevanza giuridica, attraverso una sorta di cancellazione legale della sottoscrizione.

Tale perdita di rilevanza giuridica può essere evitata solamente attraverso la conservazione a norma del documento stesso, che preceda e prevenga la scadenza dei certificati di firma utilizzati.

Una volta, invece, verificatasi detta perdita di rilevanza giuridica, essa non potrà essere recuperata ricorrendo ad un qualunque metodo di etero datazione previsto dal nostro ordinamento, ma solo attraverso metodi che, oltre ad essere previsti da una norma, siano contemporaneamente anche idonei ad attestare non tanto l’apposizione della firma in un determinato momento, quanto piuttosto l’esistenza del documento informatico nella sua interezza (e quindi con quella particolare composizione e sequenza binaria) in un determinato momento.

Ciò che deve avere data certa non è tanto la realtà storica dell’apposizione di una firma digitale, quanto piuttosto la complessiva sequenza binaria che rappresenta quel particolare documento informatico.

Eugenio Stucchi
Michele Manente
Sabrina Chibbaro