Chi ha inventato il documento informatico?

Collegio Ghislieri
17 novembre 2011

Documento informatico, ritorniamo al futuro

Manlio Cammarata - *InterLex*

L'ordinamento italiano ha iniziato a recepire il documento informatico con effetti giuridici nell'ormai lontano 1997. Nel resto del mondo c'erano già state iniziative che andavano nella stessa direzione, ma riguardavano applicazioni particolari, senza un'efficacia generale. Invece in Italia i problema venne affrontato – e risolto in linea di principio – con una visione sistematica di grande lungimiranza: al documento informatico venivano attribuite la stessa rilevanza e la stessa efficacia giuridica del documento tradizionale, in presenza di determinati requisiti.

A quella prima formulazione nel corso degli anni si è sovrapposto un numero di provvedimenti che è persino difficile contare. La materia ha raggiunto un livello di complicazione che rende arduo qualsiasi tentativo di interpretazione ed è causa di continue incertezze applicative. L'unica soluzione possibile è quella che ben conosce chi si trova di fronte a un sistema informatico bloccato: RESET!

In sostanza è necessario ritrovare i fondamenti dell'innovazione legislativa e ripartire da questi: come quindici anni fa, quando il documento informatico era il futuro: è il senso del titolo di questo intervento. Ma, attenzione: non si deve ritornare al passato, fare tabula rasa di tutto quello che è stato costruito. Gli sforzi interpretativi e l'esperienza applicativa di questi hanno sono il presupposto necessario di una "ri-costruzione" del quadro normativo. Dunque le note che seguono propongono di riconsiderare i fondamenti della materia come furono impostati all'origine e di ricostruire una visione sistematica che tenga conto degli sviluppi interpretativi e delle esperienze applicative di questi anni.

Il quadro generale si può riassumere in pochi punti molto semplici:

1. il documento informatico con effetti giuridici è indispensabile per la "dematerializzazione" delle attività amministrative e dei rapporti tra i privati;
2. il documento informatico è al centro di un sistema che comprende l'intero "ciclo di vita" delle informazioni che contiene: dunque non solo formazione, trasmissione, conservazione del documento stesso, ma anche tutte le attività che hanno il documento informatico come strumento essenziale (posta certificata, protocollo ecc.);
3. gli effetti legali sono possibili solo se i documenti informatici sono "sigillati" con procedure che ne attestino l'integrità e, quando è necessario, diano certezza legale dell'identità dei soggetti responsabili della loro formazione, trasmissione e trattamento;
4. queste procedure consistono nell'apposizione di *segnature digitali*, chiamate (con notevole imprecisione) "firme digitali" o "firme elettroniche";
5. poiché le segnature digitali sono gli strumenti essenziali per l'esistenza e per gli effetti dei documenti informatici, esse devono essere chiaramente definite nella loro

natura: in particolare si deve distinguere tra strumenti di validazione dei contenuti, strumenti di validazione delle procedure e strumenti di attribuzione della responsabilità degli atti (i soli che nel nostro ordinamento possono essere definiti "firme").

Partendo da questa base sarà possibile fare luce su una serie di equivoci, antinomie, difficoltà interpretative e applicative. E semplificare un quadro normativo ormai ingestibile nella sua complessità.

Il "triangolo" normativo

L'edificio normativo del documento informatico è sostenuto da pilastri (necessari e sufficienti):

1. la tecnologia;
2. il quadro normativo europeo;
3. il nostro ordinamento nazionale.

Possiamo quindi immaginare il sistema come inscritto in un triangolo, i cui vertici sono costituiti dai tre elementi appena elencati. La figura del triangolo non deve essere considerata una metafora casuale: come sanno tutti coloro che si occupano di costruzioni, la struttura triangolare è indeformabile. A differenza di tutte le altre, che possono essere stirate o schiacciate in varie direzioni

E il nostro deve essere un triangolo equilatero: la tecnologia è un presupposto sul quale si devono fondare le norme, e non può forzare gli aspetti giuridici; l'ordinamento nazionale deve essere compatibile con quello comunitario, ma il recepimento delle direttive non può determinare "disarmonie" nel sistema interno (principio sempre presente nelle deleghe di attuazione). Occorre quindi un perfetto equilibrio fra i tre elementi, senza che nessuno possa prevalere sugli altri.

Vediamo dunque uno per uno i tre elementi.

1. La tecnologia

Diverse tecnologie sono disponibili per la validazione dei documenti e delle transazioni. Ma la crittografia a chiave pubblica è considerata lo strumento più adatto alla creazione delle segnature digitali, firme comprese. Per la semplice verifica dell'integrità delle informazioni ci sono tecniche più semplici (per esempio, i codici di controllo), ma che in genere non possono offrire certezze legali.

Naturalmente non è questa la sede per descrivere, per l'ennesima volta, il funzionamento della crittografia a chiave pubblica. Basta ricordare che essa offre un altissimo grado di sicurezza nella verifica dell'integrità del documento e nell'identificazione del soggetto che *appare* come sottoscrittore del documento, nel caso delle firme. "Appare", non "è". Perché la certezza dell'identificazione ai fini di determinati effetti giuridici è legata ad alcuni elementi esterni alla segnatura vera e propria: la generazione per mezzo di un dispositivo sicuro, la titolarità del dispositivo in capo a un soggetto "identificato con certezza", certificata da un soggetto qualificato, e la

presunzione forte del possesso del dispositivo da parte del soggetto certificato.

Qui, come si vede, i presupposti tecnici si combinano perfettamente con quelli giuridici: la tecnologia più sicura non serve a nulla se manca la certezza legale dell'attribuzione e dell'uso esclusivo del dispositivo di firma a un determinato soggetto. Per inciso, ricordo ai tecnologi che la "certezza legale" non è una "certezza assoluta", ma una presunzione che deriva dal rispetto di determinate procedure.

Sempre ai tecnologi si deve anche ricordare che le certezze legali (oltre che tecniche) non determinano l'impossibilità di "ripudiare" una firma digitale. Nozione perversa, quella del "non ripudio", che si trova con molta frequenza nelle descrizioni degli effetti dello strumento. Al contrario, nel nostro ordinamento sono previsti diversi strumenti per il disconoscimento delle firme. Negli ordinamenti di *common law*, addirittura, non ci sono nemmeno presunzioni generali di validità delle firme.

A metà strada tra la tecnologia e il diritto (quale?) ci sono alcune regole emanate da organismi internazionali (UNCITRAL), che però non sembrano rilevanti per la costruzione del quadro normativo nazionale. Possono costituire un riferimento per la redazione delle regole tecniche.

Infine si deve ricordare ancora una volta che la trasposizione di principi tecnici in norme di diritto positivo deve essere compiuta senza creare disarmonie con l'ordinamento. È accaduto, fra l'altro, con la previsione della perdita di qualsiasi valore giuridico dei documenti informatici dopo la scadenza del certificato, introdotta dalle regole tecniche del 1999: motivata sul piano tecnico dalla (esagerata) preoccupazione che l'aumento continuo della potenza degli elaboratori possa diminuire col tempo la sicurezza delle firme, ha determinato una inaccettabile discriminazione tra il documento tradizionale e il documento elettronico. Creando più problemi di quanti se ne possano immaginare in seguito all'improbabile (perché comunque difficilissima) falsificazione di una singola firma digitale.

2. Il quadro comunitario

La normativa europea sul documento informatico è contenuta nella "direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche". A differenza della normativa italiana, il suo fine principale non è l'attribuzione di effetti giuridici ai documenti informatici, ma la costruzione di un sistema di regole comuni che faciliti l'interscambio comunitario dei documenti in formato elettronico e, soprattutto, degli strumenti e dei servizi relativi. L'equiparazione della firma digitale alla firma autografa è infatti un aspetto particolare della direttiva, dettagliato negli allegati anziché nel testo principale.

La formulazione è piuttosto confusa, dal nostro punto di vista, perché deve conciliare i principi di *civil law* con quelli di *common law*, evitando le rigidità di tipo codicistico che renderebbero più chiare le regole per gli Stati di *civil law*. Inoltre il testo è stato varato con troppa fretta: una rilettura avrebbe probabilmente migliorato molti aspetti critici.

In estrema sintesi, la direttiva contempla un solo strumento di validazione dei

documenti elettronici: la *electronic signature*. La traduzione "a orecchio" con *firma elettronica* è la causa di molti dei problemi con i quali ci misuriamo da dodici anni. Infatti la parola inglese *signature* in italiano ha molti significati, fra i quali quello di *firma* non è il solo che si adatta alla materia. Come vediamo tra un attimo, traducendo il termine nel più generico *segnatura*.

L'art. 2 della direttiva stabilisce le definizioni essenziali. In particolare, con una traduzione in italiano più aderente al contesto si legge:

1. "electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;	1. "segnatura elettronica" significa dati in forma elettronica che sono allegati o logicamente associati con altri dati elettronici e che servono come metodo di validazione;

L'assenza di qualsiasi riferimento a un soggetto a cui possa essere attribuita la segnatura esclude che possa trattarsi di una "firma" nel senso che il nostro ordinamento attribuisce a questa espressione. Come è confermato dalla definizione successiva:

2. "advanced electronic signature" means an electronic signature which meets the following requirements: *(a) it is uniquely linked to the signatory;* *(b) it is capable of identifying the signatory;* *(c) it is created using means that the signatory can maintain under his sole control; and* *(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;*	2. "segnatura elettronica avanzata" significa una segnatura elettronica che soddisfa i seguenti requisiti: a) è unicamente collegata al firmatario; b) è idonea a identificare il firmatario; c) è creata usando mezzi che il firmatario può mantenere sotto il suo esclusivo controllo; e d) è collegata ai dati ai quali si riferisce in modo che sia rilevabile qualsiasi modifica dei dati successiva [alla sua creazione];

In questa seconda definizione al termine *signature* può essere attribuito il signficato di *firma*. Il confronto tra le due definizioni conferma senza ombra di dubbio che la *electronic signature* del n. 1 non è una "firma", intesa come "segno" (*signature*) riconducibile a un soggetto identificabile.

Fino a questo punto nella direttiva manca qualsiasi accenno agli effetti giuridici delle segnature elettroniche, in particolare della *advanced*. Per non parlare dell'equivalenza alla firma autografa.

Ai nostri occhi appare singolare la definizione della firma come *species* di un generico sistema di validazione dei dati. Ma se ci poniamo in un'ottica non codicistica, il conto torna: definito "segnatura elettronica" un sistema di validazione dei dati, l'aggiunta dell'informazione tecnicamente sicura sull'identità di un firmatario rende "avanzata" la stessa segnatura elettronica.

In tutto questo, nel profluvio di "firme" che ha invaso progressivamente la nostra normativa, manca la *digital signature* prevista dalla direttiva.

Degli effetti giuridici si occupa l'art. 5:

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: *(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and* *(b) are admissible as evidence in legal proceedings.*	1. Gli Stati Membri garantiranno che le segnature elettroniche avanzate che sono basate su un certificato qualificato e che sono create da un dispositivo per la creazione di firme sicure: a) soddisfino i requisiti legali di una segnatura in relazione ai dati in forma elettronica nello stesso modo in cui una firma autografa soddisfa questi requisiti in relazione a dati basati su carta; e b) siano ammissibili come prova in giudizio.

Dunque la firma elettronica, se è basata su un certificato qualificato e generata con un dispositivo per la creazione di firme sicure, ha gli stessi effetti di una firma autografa. Punto e basta. Si noti che la firma che la nostra normativa definisce (opportunamente) come "qualificata" non ha una specifica definizione nella direttiva. È solo una ulteriore *species* della "segnatura elettronica avanzata", a sua volta *species* del *genus* "segnatura elettronica".

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is: *in electronic form, or* *not based upon a qualified certificate, or* *not based upon a qualified certificate issued by an accredited certification-service-provider, or* *not created by a secure signature-creation device.*	2. Gli Stati membri garantiranno che di una segnatura elettronica non possa essere negata la rilevanza legale e l'ammissibilità come prova in giudizio solo perché è: in forma elettronica, o non basata su un certificato qualificato, o non basata su un certificato qualificato emesso da un fornitori di servizi accreditato, o non generata con un dispositivo per la creazione di firme sicure.

Questo secondo comma, per il nostro ordinamento, è inutile. Infatti la rilevanza legale e l'ammissibilità come prova sono codificate solo per determinati tipi di documenti (in forma scritta, con sottoscrizione, con firma autenticata ecc.). Per tutti gli altri vale il principio generale del libero convincimento del giudice.

A ben guardare, il sistema è di una semplicità disarmante. Peccato che la forma poco chiara dell'intero testo, aggravata dalle imprecisioni della traduzione in italiano, determini di primo acchito una sensazione di confusione.

L'ordinamento italiano

Il legislatore italiano ha introdotto la sostanziale equivalenza della firma digitale alla firma autografa con l'art. 15, comma 2, della legge 59/97:

Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge; i criteri di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti…

Il primo regolamento, emanato con il DPR 513/97, ha stabilito come criteri di applicazione gli stessi che due anni dopo sarebbero stati fissati dalla direttiva 1999/93/CE: a) certificato qualificato, b) dispositivo per la generazione di firme sicure, c) controllo esclusivo del dispositivo da parte del titolare. L'insieme non era perfetto, ma il principio era – ed è ancora – perfettamente funzionale. In sostanza la direttiva non avrebbe avuto bisogno di specifiche disposizioni di attuazione in quanto:

a) per la firma idonea a produrre documenti validi e rilevanti a tutti gli effetti di legge(firma digitale), le disposizioni del DPR 513/97 coincidevano perfettamente con le alle prescrizioni dell'art. 5, c. 1, della direttiva e nelle regole tecniche del 1999 non c'erano sostanziali difformità dagli allegati (che di fatto "copiavano" le nostre norme);

b) le firme generiche (*advanced electronic signature*), cioè non asseverate dal certificato qualificato ecc., erano naturalmente soggette al libero convincimento del giudice. Sicché all'epoca delle prime norme non si era ritenuto di dover emanare disposizioni *ad hoc*.

c) stesso discorso per le segnature elettroniche (*electronic signature*), meri strumenti di validazione dei dati (comunque già in uso da anni in diversi campi – si pensi al codice di controllo costituito dall'ultima lettera del codice fiscale).

Invece di una "attuazione sistematica" è stato operato un "recepimento letterale", per di più basato su una traduzione sbagliata. Sicché dopo ripetute sovrapposizioni di attuazioni, si è arrivati a una situazione ingovernabile, nella quale non si capisce più nemmeno quante siano le specie di firma elettronica di rilevanza giuridica.

Ma in tanto iperattivismo normativo si è dimenticato di regolare la *electronic signature*, cioè il sistema di validazione dei soli dati. Essa è stata erroneamente classificata tra le *firme*, cioè tra i sistemi che consentono l'identificazione del firmatario. Con la conseguente difformità dalle definizioni della direttiva e il rischio di una procedura d'infrazione.

Ma non è il solo punto in cui la lettura superficiale di una traduzione imprecisa della direttiva ha determinato pasticci nella sua attuazione. Un'altra definizione "ballerina" deriva dalla trasposizione del termine inglese *authentication* (validazione, asseverazione, verifica…) nell'italiano *autenticazione* ("l'autenticazione consiste nell'attestazione da parte del pubblico ufficiale…" – art. 2703 cc). Così nella prima versione del CAD era stata inventata l'*autenticazione informatica* ("la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie al fine di garantire la sicurezza dell'accesso").

Come bislacca risposta alle critiche sollevate contro questa definizione, nella seconda versione era stato aggiunto un avverbio a casaccio ("*anche* al fine di garantire

la sicurezza dell'accesso"). Nell'ultima versione, la definizione di *identificazione informatica* ha finalmente messo a posto le cose. Ma è stata introdotta la definizione di *autenticazione del documento informatico*, che consiste in sostanza nell'associazione al documento di dati relativi all'autore e alla data. In questo modo alcune semplici informazioni, senza alcun requisito di certezza, sono definite come l'atto di un pubblico ufficiale.

Un altro esempio, tra i tanti possibili: il primo comma dell'art. 65 del vigente Codice recita:

> 1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:
>
> a) se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;
>
> […]

Ora, nelle definizioni dell'art. 1 si legge che la firma digitale è "un particolare tipo di firma elettronica avanzata basata su un certificato qualificato" e che il certificato qualificato è "il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva". La prima osservazione è l'inutilità della specificazione "il cui certificato è rilasciato da un certificatore accreditato", poiché il requisito è contenuto nelle definizioni (ma l'intero Codice è zeppo di queste inutili precisazioni). Ma nelle stessa definizione c'è la stranezza del richiamo alla direttiva, invece che alle disposizioni corrispondenti presenti nello stesso decreto legislativo o nelle regole tecniche.

Ma è naturale chiedersi perché le istanze e le dichiarazioni non possano essere sottoscritte con la *firma elettronica qualificata* invece che con la firma digitale: la prima, poiché corrisponde alla definizione delle *advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device*, deve avere gli stessi effetti della firma autografa e quindi essere idonea a validare l'atto.

Qual è dunque la differenza sostanziale tra la firma elettronica qualificata e la firma digitale, variamente richiamate nel CAD? La prima è "un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma"; mentre la seconda è "un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici".

Dal che si deduce che la firma elettronica qualificata non consente di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico. In altri termini: se la firma digitale è una *species* della firma elettronica qualificata, e si

distingue da questa anche perché consente di rendere manifesta e di verificare la provenienza e l'identità di un documento informatico, si deduce che questa caratteristica manca nella prima. È quanto risulta "dal significato proprio delle parole secondo la connessione di esse". La conclusione paradossale è che la firma qualificata non soddisfa i criteri della *advanced electronic signature* della direttiva.

Ci fermiamo qui, perché non basterebbe un libro per elencare e descrivere tutte le anomalie e le antinomie del testo. Per restare agli aspetti più generali, un ultimo esempio riguarda il già citato mancato recepimento del mezzo di validazione dei dati (*electronic signature*). Ha fra le altre conseguenze una "disarmonia" sul regime delle fatture commerciali. Che non devono essere firmate se in forma cartacea, mentre il fisco pretende che siano provviste di firma digitale se in forma elettronica.

A questo punto dovrebbe essere chiaro perché è necessario "ritornare al futuro", cioè ripartire dai presupposti essenziali del "triangolo" descritto all'inizio di queste note e riscrivere la normativa sul documento informatico. Ulteriori novellazioni non farebbero altro che rendere ancora più complicata la materia.