SEZIONE I
PARTE GENERALE

1. Introduzione

Il diritto può essere suddiviso in due macrocategorie: sostanziale (costituito dal complesso di norme vigenti in un ordinamento per regolare i rapporti tra le parti) e processuale (costituito da ulteriori norme finalizzate a garantire il ripristino di una situazione di legittimità, nell'ipotesi di violazione delle norme sostanziali).

Le definizioni appena proposte – come altre che seguiranno – hanno il solo scopo di introdurre i concetti che verranno svolti nel prosieguo della trattazione; esse, quindi, non sono e non voglio essere esaustive, e non sostituiscono quelle più precise offerte nell'ambito dei vari insegnamenti del diritto.

Il processo, giuridicamente inteso, è un complesso di norme che regolano i rapporti tra le parti di una controversia, disciplinano i mezzi e le modalità di raccolta e presentazione delle prove e definiscono le attività dell'autorità giudicante e dei suoi ausiliari, al fine di assicurare la corretta trattazione della lite e la sua decisione.

Poiché le controversie che possono insorgere sono della più svariata natura, alle norme processuali generali se ne aggiungono altre, più specifiche, applicabili in determinate materie (ad esempio, nel diritto del lavoro) o in presenza di alcuni presupposti (ad esempio, di prova scritta di un credito o di urgenza nella tutela di un diritto).

Nel caso in cui tali norme processuali speciali siano funzionali a specifiche materie e siano applicabili solo ad esse si parla di *riti* quali, in ambito civile, il rito processuale del lavoro, il rito processuale delle locazioni ed altri.

Il *processo telematico* – che verrà trattato in prosieguo con particolare riferimento a quello civile ove non diversamente precisato – non è un tipo di processo diverso, né introduce un nuovo rito a quelli esistenti; in altre parole: non è una nuova *specie* di processo.

Al contrario il *processo telematico* raccoglie il complesso di norme destinate a disciplinare la formazione, conservazione e comunicazione di atti e documenti tra gli attori del giudizio e tra questi ed il sistema informatico giudiziario con l'utilizzo di sistemi informatici e reti di comunicazione telematiche.

In altre parole: il *processo telematico* non è una disciplina giuridica autonoma, ma un modo di fare processo con mezzi specifici quali, come detto, i sistemi informatici e le reti di comunicazione telematiche.

2. Il documento informatico, l'opponibilità ai terzi, la firma digitale

SOMMARIO: 2.1. Bit e byte. – 2.2. Documento tradizionale e documento informatico. – 2.3. Le norme di riferimento. – 2.4. Le tipologie di firma elettronica. – 2.5. La crittografia: la base della firma digitale. – 2.6. La firma digitale. – 2.7. Il Prestatore di servizi fiduciari qualificato (ex Certificatore). – 2.8. Il dispositivo di firma digitale. – 2.9. La firma remota. – 2.10. Firma digitale e firma tradizionale: differenze. – 2.11. Le funzioni della firma: indicativa, dichiarativa e probatoria. – 2.12. I tipi di firma digitale: CAdES e PAdES.

2.1. Bit e byte

Non vi sarebbe processo telematico senza l'impiego del documento informatico e della firma digitale.

La conoscenza di questi due elementi e la consapevolezza delle loro caratteristiche e funzioni è quindi indispensabile alla comprensione del processo telematico.

I dispositivi elettronici (computer, tablet, smartphone, ecc.), che sempre di più pervadono il nostro quotidiano, sono «elaboratori» che eseguono istruzioni basate su un sistema numerico binario (detto anche «codice binario» o «sistema binario»), inventato dal matematico tedesco Gottfried Wilhelm Leibniz (Lipsia 21 giugno 1646-Hannover il 14 novembre 1716), ma in allora non sviluppato perché privo di applicazioni pratiche.

Esso verrà riscoperto dal matematico inglese George Boole (Lincoln, 2 novembre 1815-Ballintemple, 8 dicembre 1864), che aprirà l'orizzonte alle grandi scuole di logica matematica del '900 favorendo la nascita del calcolatore elettronico.

Come il nome suggerisce il codice binario utilizza due simboli, tipicamente 0 e 1, invece dei 10 del sistema decimale tradizionale; è un sistema numerico posizionale in base 2.

Nel linguaggio dei computer non sono ammesse altre entità diverse da queste, che rappresentano l'unità minima, indivisibile, dell'informatica: il «bit» (dalla crasi delle parole BInary digiT, cioè elemento binario).

L'impiego di due bit (0 e 1) non consente, evidentemente, di rappresentare tutte le unità necessarie, ad esempio, per la comunicazione tra soggetti.

Infatti, quando scriviamo un documento utilizziamo un numero consistente di simboli grafici (lettere dell'alfabeto, numeri, segni di punteggiatura, accentate, ecc.).

Al contrario, nel codice binario, sono realizzabili solo quattro combinazioni (00, 01, 10, 11) e questo perché la numerazione del codice binario è – come detto – in base due (consente, cioè, l'impiego di due soli valori: lo zero e l'uno), vale a dire: 2^2.

Quindi – semplificando al massimo e scusandoci per l'improprietà di linguaggio – possiamo dire che per aumentare il numero di combinazioni e riuscire a rappresentare una quantità sufficiente di elementi (quali, nell'esempio fatto, le lettere dell'alfabeto, i numeri, le accentate ed i segni di punteggiatura) è necessario che la potenza alla quale elevare la base due sia superiore a due (2^2) ed abbastanza grande per conseguire il risultato desiderato.

Tale potenza è 8 che, applicata alla base due (2^8), dà un risultato di 256.

La combinazione di 8 bit (che prende il nome di byte) consente – in tutte le variazioni possibili (00000001, 00000010, 00000011 ... sino a ... 11111111) – la rappresentazione di 256 diversi elementi.

Non è il caso, in questa sede, di approfondire ulteriormente l'argomento, essendo sufficiente aver fatto comprendere che il «linguaggio macchina» alla base dell'informatica è assolutamente diverso da quello tradizionalmente usato nelle comunicazioni tra soggetti.

2.2. Documento tradizionale e documento informatico

Secondo l'insegnamento di Carnelutti bisogna tenere distinto il contenuto (atto) dal contenitore (documento).

Nella quotidianità percepiamo un atto (ad esempio: un contratto, una lettera, ecc.) tramite l'elemento (normalmente cartaceo) sul quale esso è rappresentato: il documento, per l'appunto.

L'avvento dell'informatica e l'utilizzo sempre maggiore degli strumenti da essa forniti impongono qualche riflessione.

Infatti, la materialità del documento viene sempre meno, fino a poter mancare del tutto.

Pensiamo a quello che accade nel commercio telematico che si realizza con la trasmissione a distanza di ... bit (o meglio byte).

Qual'è il documento originale e, soprattutto, dove si trova? È il file prodotto dal mittente e conservato nel suo computer o piuttosto quello ricevuto e trattenuto dal destinatario?

Andiamo per gradi.

Innanzi a tutto, va chiarito che un documento informatico è un insieme di bit che, in linguaggio macchina, appaiono come una serie di 0 e 1 privi di spazi, senza soluzione di continuità; ciò perché un documento informatico è, nella sostanza, una raccolta di «istruzioni» leggibili dal processore del computer (o da altro dispositivo informatico quali: tablet, smartphone, ecc.).

Per rendere intelligibile all'uomo un documento informatico sono necessarie delle interfacce: software (ad esempio un programma di videoscrittura) ed hardware (monitor e stampante *in primis*).

Il documento informatico è impalpabile e ciò perché è costituito – come abbiamo scritto – da «istruzioni informatiche» interpretate dai dispostivi informatici.

Inoltre, il documento informatico prescinde dal supporto sul quale esso è conservato (hard disk, floppy disk, CD, DVD, disco ottico, chiavetta USB, ecc.).

E poiché il documento – secondo la moderna teoria giuridica inaugurata dal Carnelutti – è l'elemento che consente di trasmettere la conoscenza di qualcosa (contenuta nel documento stesso), è evidente che nessuna differenza può essere fatta a seconda del supporto sul quale il documento stesso è stato redatto, con conseguente assoluta assimilabilità del documento cartaceo a quello informatico.

Il Codice dell'Amministrazione Digitale (CAD), contenuto nel D.Lgs. 7 marzo 2005, n. 82, al quale faremo spesso richiamo nel corso della nostra trattazione, offre le seguenti definizioni:

- *documento informatico*: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, lett. p);
- *documento analogico*: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, lett. p-*bis*).

Posto questo, dobbiamo ancora precisare che ciò che qui interessa non è il «documento informatico» astrattamente inteso (ed in ordine al quale potremmo anche ritenere di aver già detto tutto l'essenziale), vale a dire il mero insieme di informazioni che possono essere scambiate telematicamente, bensì il documento con rilevanza giuridica, come le promesse unilaterali (di acquisto, ad esempio), le offerte al pubblico, i contratti, gli atti del processo, ecc.

A tal fine è essenziale l'attribuzione ad un soggetto della paternità del documento, intesa non come mera individuazione del suo autore, bensì quale assunzione degli effetti giuridici del contenuto del documento.

Tale risultato, nel documento tradizionale, si ottiene con la sottoscrizione.

Non diversamente in quello informatico che, per le sue peculiari caratteristiche, comporta delle differenze.

Infatti, ai fini sopra illustrati, la firma del documento informatico non può consistere nella semplice acquisizione del segno grafico, costituente la sottoscrizione di un soggetto, e la sua riproduzione in calce al documento stesso.

E la ragione è di tutta evidenza. Nelle comunicazioni telematiche ciò che viene trasmesso è un insieme di byte, chi li riceve non ha, ne può avere, la certezza di chi glieli ha trasmessi, ben potendo il mittente essere soggetto diverso da quello apparente, al quale non sarebbe certamente opponibile il «segno grafico» rappresentativo della sua firma, che ben potrebbe essere stato acquisito (ad esempio, tramite uno scanner) a sua insaputa.

Inoltre, il contenuto del documento informatico potrebbe essere stato alterato; anche di questo il destinatario non se ne renderebbe conto, come invece accade (o dovrebbe accadere) nel caso di impiego del tradizionale documento cartaceo.

Ad evitare il rischio di alterazioni indesiderate di un documento informatico soccorrono le firme elettroniche: avanzata, qualificata e digitale, delle quali diremo in prosieguo, con particolare riferimento alla firma digitale, in quanto di uso prevalente se non esclusivo nel *processo telematico*.

2.3. Le norme di riferimento

La diffusione e l'utilizzo degli strumenti informatici hanno imposto di trovare soluzione ai problemi connessi al passaggio dal sistema tradizionale, basato sulla documentazione cartacea, a quello nuovo «informatico».

Il legislatore ha introdotto nell'ordinamento italiano la disciplina del documento informatico in tre fasi successive:

- Dapprima, con l'art. 15, comma 2, Legge 15 marzo 1997, n. 59 che ha enunciato il principio secondo il quale: «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. ...», demandando ad un successivo specifico regolamento «i criteri e le modalità di applicazione del presente comma».
- Quindi, con il D.P.R. 10 novembre 1997, n. 513 contenente il «Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art. 15, comma 2 della Legge 15 marzo 1997, n. 5» che ha rinviato ad un successivo «decreto del Presidente del Consiglio dei Ministri, da emanare entro centottanta giorni dalla data di entrata in vigore del (predetto) regolamento, sentita l'Autorità per l'informatica nella pubblica amministrazione (il compito) di fissa(re) le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici.» (art. 3, comma 1, D.P.R. n. 513/1997).

- Infine, con il Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 pubblicato sulla *Gazzetta Ufficiale* del 15 aprile 1999, n. 87 di attuazione del D.P.R. 10 novembre 1997, n. 513 contenente le «Regole tecniche per la formazione, la trasmissione, la conservazione la duplicazione, la riproduzione, la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1» del citato D.P.R.

Con D.P.R. 28 dicembre 2000, n. 445 è stato adottato il *testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa* che ha abrogato il D.P.R. n. 513/1997 (art. 77), del quale ha pressoché integralmente recepito il contenuto.

Tale testo unico è poi stato in ampia parte abrogato dal D.Lgs. 7 marzo 2005, n. 82 – Codice dell'Amministrazione Digitale (CAD) –, modificato dal D.Lgs. 27 agosto 2016, n. 179, con effetti dal 14 settembre 2016.

L'Italia è stato uno dei primi paesi al mondo ad avere recepito nel proprio ordinamento una così importante innovazione tecnologica, introducendo (tra le altre firme elettroniche) la firma digitale, per conferire validità giuridica al documento informatico, come negli vedremo in prosieguo.

La firma digitale non è qualcosa di riconducibile ad un elemento materiale immediatamente percepibile – così come la firma tradizionale –, essendo invece un sistema di cifratura e decifratura a chiavi asimmetriche (detto anche a chiave pubblica), idoneo a garantire la certezza della genuinità e della provenienza dei documenti informatici.

Il CAD (D.Lgs. n. 82/2005) – e prima ancora il T.U. n. 445/2000 ed il D.P.R. n. 513, 10 novembre 1997, n. 513 – equipara la firma digitale a quella tradizionale disponendo che:

- «Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, ha altresì l'efficacia prevista dall'art. 2702 c.c. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria. Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa anche regolamentare in materia di processo telematico.» (art. 21, comma 2).
- «Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata o digitale.» (art. 21, comma 2-*bis*).

Stante l'equivalenza, sul piano giuridico, della firma digitale a quella tradizionale e dei particolari effetti che ciò comporta, è ora opportuno domandarsi come la prima possa assolvere alle funzioni attribuite dalla dottrina alla seconda e precisamente:

- *funzione indicativa* dell'autore del documento, consistente nella possibilità di risalire con certezza all'identità del sottoscrittore;
- *funzione dichiarativa* di approvazione del contenuto del documento da parte del sottoscrittore, consistente nell'assunzione della paternità delle dichiarazioni in esso rese; il documento potrebbe, infatti, essere stato redatto da altri, ma è solo colui che lo sottoscrive che si assume la responsabilità delle dichiarazioni in esso contenute come manifestazione della propria volontà;
- *funzione probatoria* che è il risultato delle due funzioni precedenti costituendo mezzo di prova della provenienza delle dichiarazioni contenute nel documento da chi l'ha sottoscritto.

2.4. Le tipologie di firma elettronica

La firma digitale, di cui tratteremo in prosieguo, è un particolare tipo di firma elettronica ed è quella che offre il massimo grado di sicurezza.

L'Italia, a differenza di altri paesi europei, ha costruito la disciplina della sottoscrizione dei documenti informatici intorno alla firma digitale che, in origine, era l'unica che poteva attribuire validità al documento informatico, consentendone l'opponibilità ai terzi.

Il 19 gennaio 2000 veniva pubblicata nella Gazzetta Ufficiale della Comunità Europea (G.U.C.E. 19 gennaio 2000, n. L 13), la Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche.

Nei «considerando» [1] di tale direttiva venivano indicati una serie di principi tra i quali:

- i «criteri armonizzati relativi agli effetti giuridici delle firme elettroniche manterranno un quadro giuridico coerente in tutta la Comunità; il diritto nazionale stabilisce differenti requisiti per la validità giuridica delle firme autografe; i certificati possono essere usati per confermare l'identità di una persona che ricorre alla firma elettronica; le firme elettroniche avanzate ba-

[1] Le Direttive ed i Regolamenti europei iniziamo con l'elencazione dei «considerando» che costituiscono le premesse ed illustrano i principi e gli obiettivi da perseguire; dopo i «considerando» vi sono gli articoli della Direttiva ovvero del Regolamento al cui rispetto sono tenuti tutti gli Stati dell'Unione Europea.

sate su un certificato qualificato mirano ad un più alto livello di sicurezza; le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura possono essere considerate giuridicamente equivalenti alle firme autografe solo se sono rispettati i requisiti per le firme autografe» (considerando n. 20 direttiva);

- «al fine di contribuire all'accettazione generale dei metodi di autenticazione elettronici, è necessario garantire che le firme elettroniche possano essere utilizzate come prove nei procedimenti giudiziari in tutti gli Stati membri; il riconoscimento giuridico delle firme elettroniche dovrebbe basarsi su criteri oggettivi e non essere connesso ad un'autorizzazione rilasciata al prestatore di servizi di certificazione interessato; il diritto nazionale disciplina la definizione dei campi giuridici in cui possono essere impiegati documenti elettronici e firme elettroniche; la presente direttiva lascia impregiudicata la facoltà degli organi giurisdizionali nazionali di deliberare in merito alla conformità rispetto ai requisiti della presente direttiva e non lede le norme nazionali in materia di libero uso delle prove in giudizio» (considerando n. 21 direttiva).

L'Italia recepiva la Direttiva 1999/93/CE con D.Lgs. 23 gennaio 2002, n. 10, modificando il T.U. n. 445/2000 e riconoscendo la validità ed efficacia nel nostro paese di vari tipi di firma elettronica oltre a quella digitale.

La Direttiva 1999/93/CE è, poi, stata abrogata e sostituita dal Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014, denominato Regolamento eIDAS, che ha comportato la modifica di alcuni articoli del CAD.

I *tipi di firma elettronica* attualmente vigenti sono:

- «firma elettronica», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (art. 3, n. 10, Regolamento eIDAS, richiamato dall'art 1-*bis* del CAD);
- «firma elettronica avanzata», una firma elettronica che soddisfi i requisiti di cui all'art. 26 del Regolamento eIDAS (art. 3, n. 11, Regolamento eIDAS, richiamato dall'art. 1-*bis* del CAD);
- «firma elettronica qualificata», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche (art. 3, n. 12, Regolamento eIDAS, richiamato dall'art. 1-*bis* del CAD);
- «firma digitale»: un particolare tipo di firma qualificata basata 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 (art. 1, lett. s, CAD).

Dalle definizioni e dai richiami operati dalla normativa nazionale al Regolamento europeo eIDAS traiamo quale conclusione che i primi tre tipi di firma esistono in tutti i paesi dell'Unione Europea (ovvero esisteranno in quei paesi che ancora non li hanno adottati/riconosciuti), mentre la firma digitale è un tipo di firma che l'ordinamento italiano ha aggiunto.

Le firme elettroniche sono classificate nelle seguenti tre categorie: «qualcosa che conosci» (*something you know*), «qualcosa che sei» (*something you are*), e «qualcosa che hai» (*something you have*), a seconda che la procedura di autenticazione si basi sulle conoscenze dell'utente (quali una parola o un numero di identificazione personale), sulle sue caratteristiche fisiche (quale l'impronta digitale) o sul possesso di un oggetto (come una smart card od un dispositivo usb).

Tale classificazione non definisce le caratteristiche tecniche dei metodi di autenticazione, così come il livello di sicurezza.

Il livello di sicurezza delle firme elettroniche – con riflessi sulla loro giuridica valenza – va da quello minimo della firma elettronica a quello massimo della firma digitale.

La *firma elettronica* costituisce il livello minimo di sicurezza ed è definita anche «firma elettronica semplice» o «firma elettronica debole». Essa si riduce, ad esempio, al mero utilizzo di user e pass in possesso dell'utente (note come «credenziali di accesso»). In altre parole, quando accediamo ad un sito internet nel quale siamo registrati ovvero avviamo il nostro browser di posta elettronica digitando le nostre credenziali noi apponiamo la nostra «firma elettronica». Altri esempi di firma elettronica semplice sono la firma biometrica (sempre più spesso in uso presso gli sportelli bancari che presentano un tablet ove il correntista appone la firma) ovvero il PIN di una carta di credito.

La *firma elettronica avanzata* deve soddisfare i seguenti requisiti:

a) essere connessa unicamente al firmatario;
b) essere idonea a identificare il firmatario;
c) essere creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e
d) essere collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

In buona sostanza: la firma elettronica avanzata viene rilasciata previa identificazione del futuro utilizzatore (a differenza di ciò che accade nella firma elettronica semplice ove può accadere che sia l'utente stesso ad autodichiararsi), garantisce la connessione univoca tra il firmatario e il documento ed è creata con mezzi sui quali quest'ultimo ha un controllo esclusivo. L'associazione della firma elettronica avanzata al documento comporta la possibilità di rilevarne l'eventuale alterazione (come spiegheremo oltre).

La *firma elettronica qualificata* è una firma elettronica avanzata che può essere generata solo impiegando uno specifico dispositivo di firma[2] che garantisce la sicurezza e la non contraffazione della firma ed è basata su un certificato qualificato consistente in un attestato elettronico, rilasciato da un prestatore di servizi fiduciari (anche di questo diremo oltre), che collega i dati di convalida di una firma elettronica ad una persona fisica confermandone il nome o lo pseudonimo.

La *firma digitale* è un firma elettronica qualificata basta su un sistema di cifratura a chiavi asimmetriche.

A seconda del tipo di firma utilizzato, diversa è l'efficacia del documento al quale essa è associata.

Il documento informatico firmato con firma elettronica semplice è liberamente valutabile dal giudice ai sensi dell'art. 21, comma 1 del CAD.

Il documento informatico firmato con firma elettronica avanzata è equiparato alla scrittura privata sottoscritta, quindi fa piena prova delle dichiarazioni contenute nel documento stesso contro colui che l'ha firmato; essa non è utilizzabile nei contratti immobiliari. In altre parole, integra la forma scritta *ad substantiam*, tranne che per i contratti immobiliari ove è richiesta una firma elettronica di livello superiore (art. 21, comma 2 del CAD).

Il documento informatico firmato con firma elettronica qualificata o firma

---

[2] L'allegato II del Regolamento eIDAS così definisce le caratteristiche che devono avere i dispositivi di firma elettronica qualificata.

1. I dispositivi per la creazione di una firma elettronica qualificata garantiscono, mediante mezzi tecnici e procedurali appropriati, almeno quanto segue:

a) è ragionevolmente assicurata la riservatezza dei dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica;

b) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica possono comparire in pratica una sola volta;

c) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica non possono, con un grado ragionevole di sicurezza, essere derivati e la firma elettronica è attendibilmente protetta da contraffazioni compiute con l'impiego di tecnologie attualmente disponibili;

d) i dati per la creazione di una firma elettronica utilizzati nella creazione della stessa possono essere attendibilmente protetti dal firmatario legittimo contro l'uso da parte di terzi.

2. I dispositivi per la creazione di una firma elettronica qualificata non alterano i dati da firmare né impediscono che tali dati siano presentati al firmatario prima della firma.

3. La generazione o la gestione dei dati per la creazione di una firma elettronica per conto del firmatario può essere effettuata solo da un prestatore di servizi fiduciari qualificato.

4. Fatto salvo il punto 1, lettera d), i prestatori di servizi fiduciari qualificati che gestiscono dati per la creazione di una firma elettronica per conto del firmatario possono duplicare i dati per la creazione di una firma elettronica solo a fini di back-up, purché rispettino i seguenti requisiti:

a) la sicurezza degli insiemi di dati duplicati deve essere dello stesso livello della sicurezza degli insiemi di dati originali;

b) il numero di insiemi di dati duplicati non eccede il minimo necessario per garantire la continuità del servizio.

digitale è equiparato alla scrittura privata sottoscritta e quindi fa piena prova delle dichiarazioni contenute nel documento informatico contro colui che l'ha firmato ed è utilizzabile senza limitazione (la firma, come vedremo, si produce utilizzando una smart-card o un token) – art. 21, comma 2-*bis* del CAD –.

2.5. La crittografia: la base della firma digitale

Dopo avere illustrato i tipi di firma elettronica e la graduazione della loro efficacia, entriamo nel merito della firma digitale.

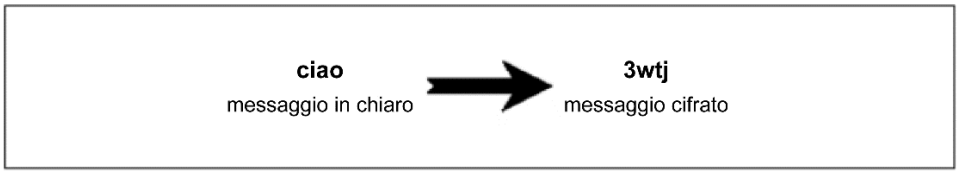
Per rispondere al quesito che ci siamo posti sulla validità giuridica del documento informatico firmato con firma elettronica, in particolare digitale, è necessario spiegare, nel modo più semplice e meno tecnico possibile, il sistema crittografico alla base della firma digitale.

Facciamo un esempio.

Supponiamo che Andrea debba trasmettere a Grazia un documento che non vuole che altri possano leggere.

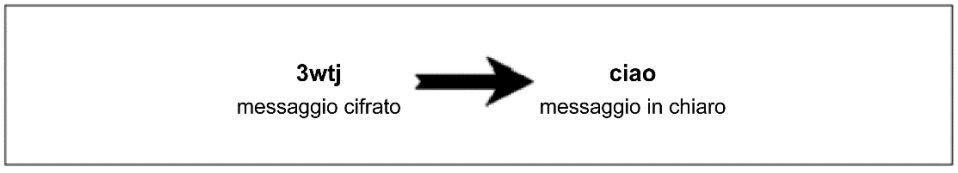
La strada da seguire è quella della crittografia, vale a dire di quella tecnica che, applicando un algoritmo ad una serie di caratteri alfanumerici intellegibili a chiunque, li rende incomprensibili.

Figura 01



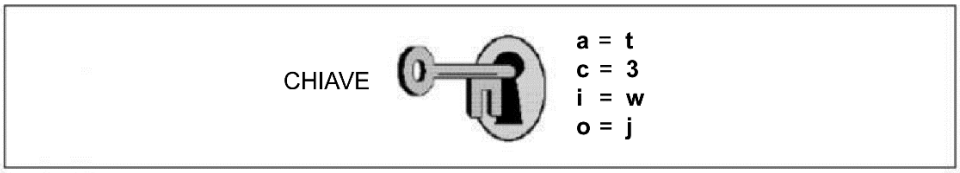
Naturalmente, il processo di crittografia deve essere reversibile e consentire, quindi, di rendere intellegibile il documento precedentemente criptato.

Figura 02



L'elemento che consente di criptare e decriptare un documento è chiamato «chiave».

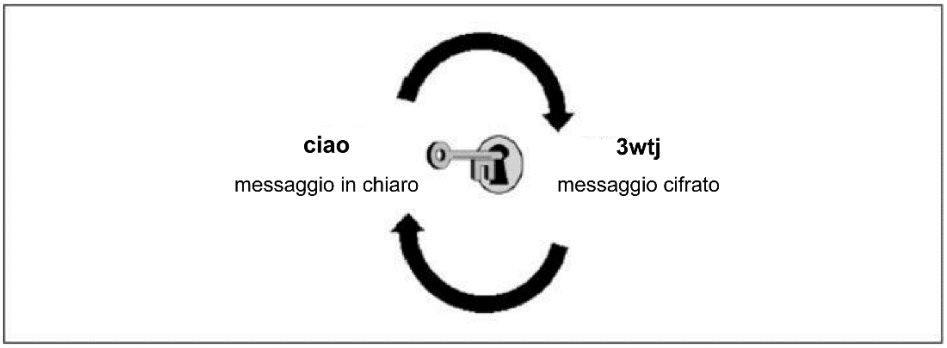
Figura 03



I *sistemi di crittografia* sono di due tipi: quello *simmetrico*, detto anche a *chiave segreta* e quello *asimmetrico*, denominato anche a *chiave pubblica*.

Nel *sistema simmetrico* si usa la medesima chiave sia per criptare che per decriptare; ecco la ragione per la quale la chiave deve essere segreta.

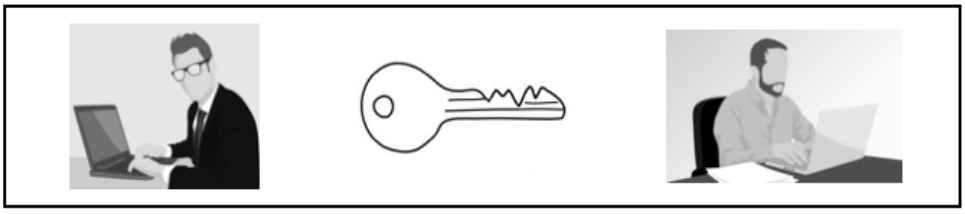
Figura 04



L'uso di questo sistema importa alcune *controindicazioni e problemi* quali:

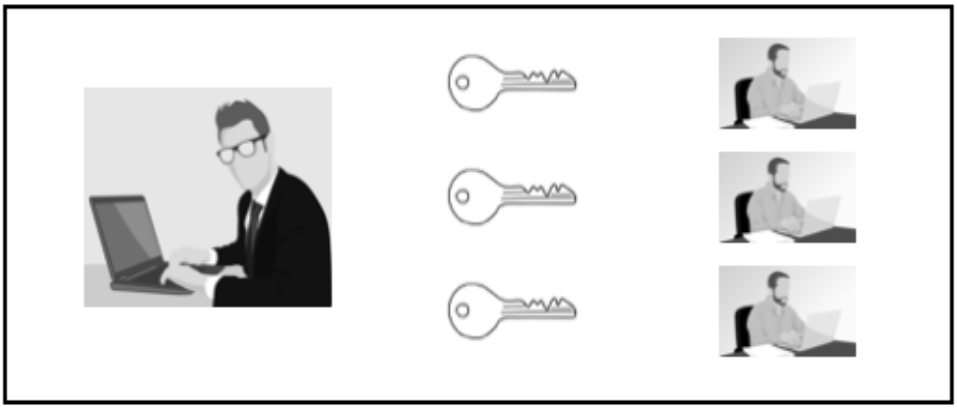
- la necessità di trasmettere al destinatario la chiave segreta da impiegare per decifrare il documento, con conseguente rischio nella sicurezza della trasmissione di tale chiave, che se entrasse in possesso di terzi annullerebbe gli effetti della cifratura e non consentirebbe di considerare segreto il documento criptato;

Figura 05



- l'impossibilità di assicurare, nei rapporti tra mittente e destinatario, la genuinità del documento; il destinatario, disponendo della chiave segreta del mittente, potrebbe alterare il documento originario per poi ricifrarlo ed utilizzarlo in ulteriori comunicazioni con altri soggetti, spacciandolo per autentico e di provenienza dell'apparente autore;
- l'oggettiva difficoltà di possedere, gestire e trasmettere una pluralità di chiavi segrete nell'ipotesi di comunicazioni riservate con più destinatari.

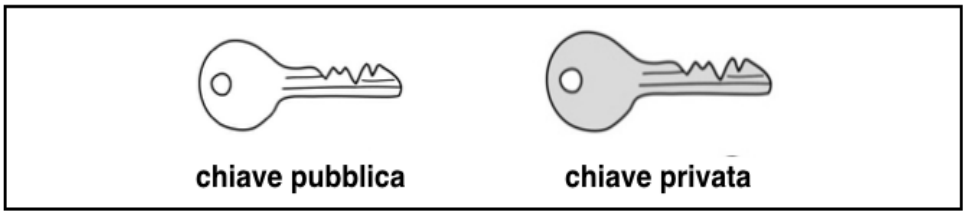
Figura 06



Tali problemi non si pongono nel *sistema asimmetrico* o a chiave pubblica.

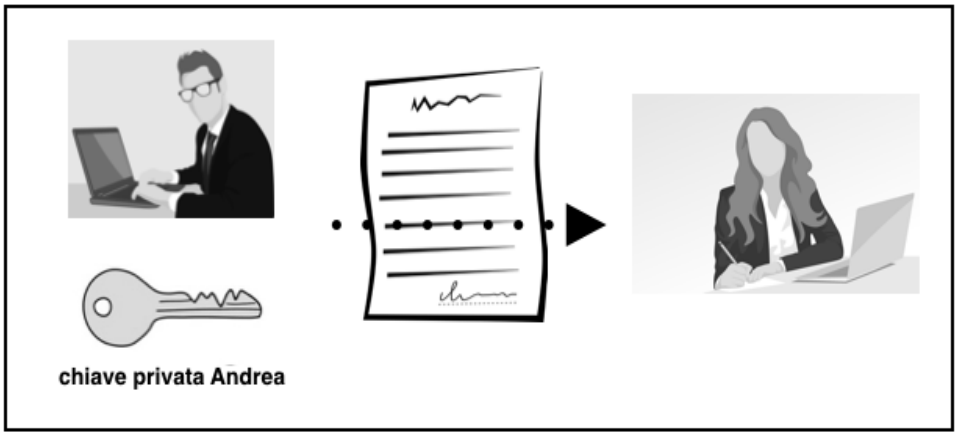
In tale sistema, infatti, per la cifratura e la decifratura dei documenti sono necessarie due chiavi, diverse tra loro, delle quali, una rimane segreta e nella disponibilità esclusiva del solo titolare, mentre la seconda è, per l'appunto, pubblica e, quindi, conosciuta ovvero conoscibile da chiunque, perché annotata in appositi registri tenuti da un soggetto terzo (in origine definito «certificatore») che garantisce l'identità del soggetto titolare di tale chiave.

Figura 07



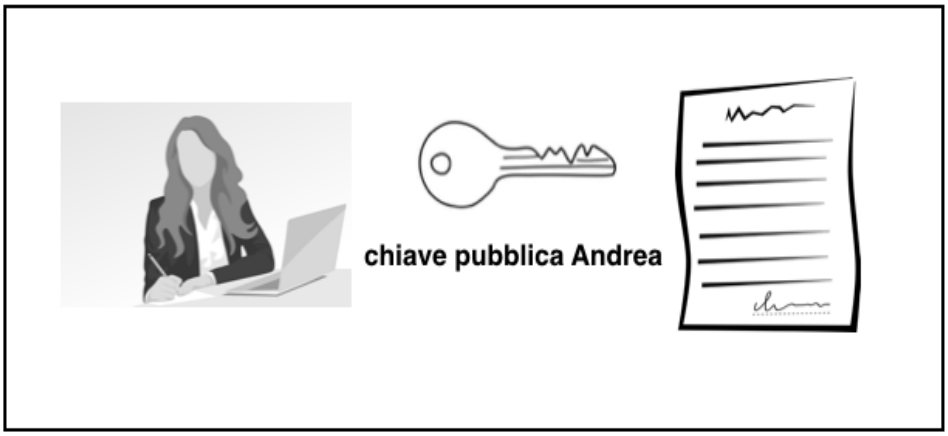
Per cui, nell'esempio proposto, il mittente (Andrea) cifrerà il documento con la propria chiave privata (segreta) e lo trasmetterà al destinatario (Grazia).

Figura 08



Grazia utilizzerà – poi – la chiave pubblica di Andrea per decifrarlo.

Figura 09



Così operando Andrea non dovrà mai trasmettere la propria chiave privata che, quindi, rimarrà segreta.

Grazia, a sua volta, dopo aver decifrato il documento ricevuto utilizzando la chiave pubblica di Andrea, avrà la certezza che il documento è genuino e che proviene da Andrea.

In altre parole: un documento cifrato con una determinata chiave privata potrà essere decifrato solo con la corrispondente chiave pubblica.

Vale, evidentemente, anche la regola inversa; per cui un documento deci-

frato con una determinata chiave pubblica non potrà essere stato cifrato che con la corrispondente chiave privata.

Il sistema delle chiavi asimmetriche assicura la paternità del documento, vale a dire l'identità del mittente e la sua integrità, quindi la non ripudiabilità dello stesso.

Rimane – però – il problema della segretezza.

Infatti, se per la decifratura di un messaggio cifrato con una chiave privata è necessaria e sufficiente la chiave pubblica accessibile a chiunque, il documento cifrato è, per definizione, esso stesso pubblico o, quantomeno, può essere reso intellegibile a tutti.

Il sistema a chiavi asimmetriche offre la soluzione al problema, essendo sufficiente invertire l'uso delle chiavi sopra indicato, di modo che il mittente (Andrea) cifrerà il messaggio utilizzando la chiave pubblica del destinatario (Grazia) che sarà l'unico soggetto in grado di leggerlo, perché titolare della corrispondente chiave privata.

Riassumendo: per assicurare l'identità del mittente e la genuinità del documento il mittente cifrerà con la propria chiave privata, mentre il destinatario decifrerà con la corrispondete chiave pubblica; per assicurare la segretezza del documento il mittente cifrerà con la chiave pubblica del destinatario che decifrerà con la propria chiave privata.

Le due funzioni possono – poi – essere combinate per assicurare tanto la paternità e genuinità del documento quanto la sua riservatezza.

Per ottenere tale risultato sarà necessaria un doppia crittazione per cui il mittente (Andrea) cifrerà il documento utilizzando la propria chiave privata e – poi – lo cifrerà una seconda volta impiegando la chiave pubblica di Grazia.

Grazia, da parte sua, decifrerà il messaggio dapprima con la propria chiave privata e, subito dopo, con la chiave pubblica di Andrea.

2.6. La firma digitale

Quello appena illustrato è il sistema di crittografia dell'intero documento.

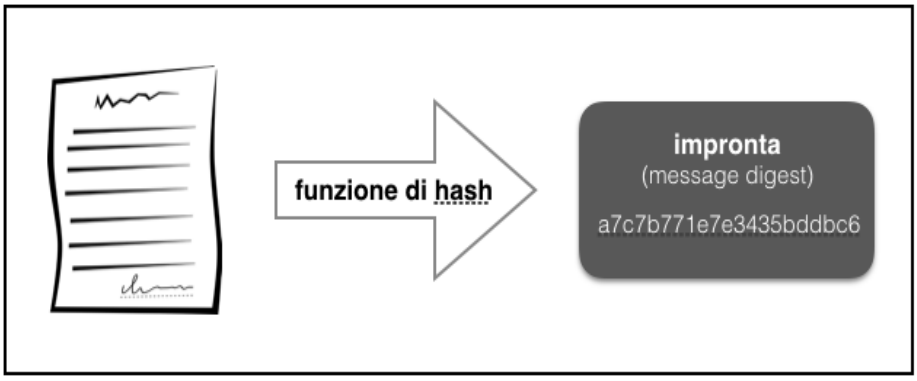
La firma digitale, pur basandosi sullo stesso principio, è qualcosa di diverso.

La cifratura di un intero documento richiede, infatti, molto tempo e potrebbe non interessarci, magari perché non abbiamo bisogno di trasmettere un messaggio riservato ma solo di garantire al destinatario (Grazia) la genuinità e la paternità del nostro documento.

In tale condizione soccorre la firma digitale che funziona nel modo che di seguito descriviamo.

a) Dopo avere redatto (*rectius* digitato) un testo, applichiamo una particolare *funzione*, detta di *hash*, che ha quale unico scopo quello di ridurre l'intero documento ad una specie di riassunto estremamente sintetico (tecnicamente: una stringa binaria di lunghezza costante di 160 bit corrispondente a 20 byte, vale a dire 20 caratteri alfanumerici) che rappresenta l'«*impronta*» (o *message digest*) del documento.

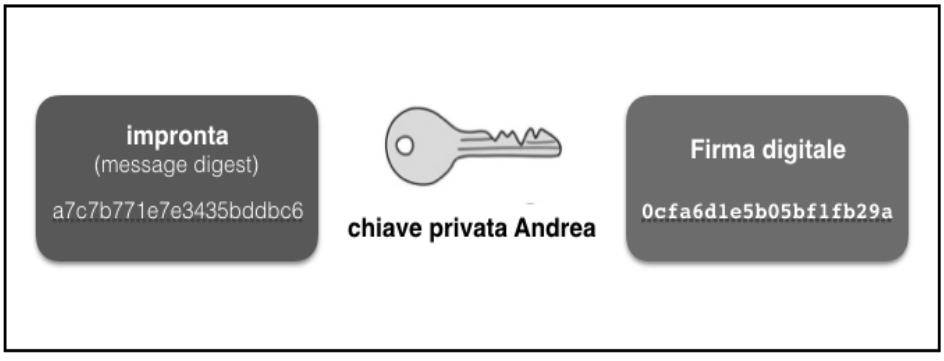
Figura 10



L'importanza della funzione di *hash* è data dal fatto che la sua applicazione assicura *l'unicità* dell'«impronta» generata, nel senso che se al testo originario modificassimo anche un solo carattere il risultato della funzione di *hash* sarebbe un'impronta diversa.

b) Applichiamo all'impronta la nostra chiave privata ed otterremo la *firma digitale* del documento.

Figura 11



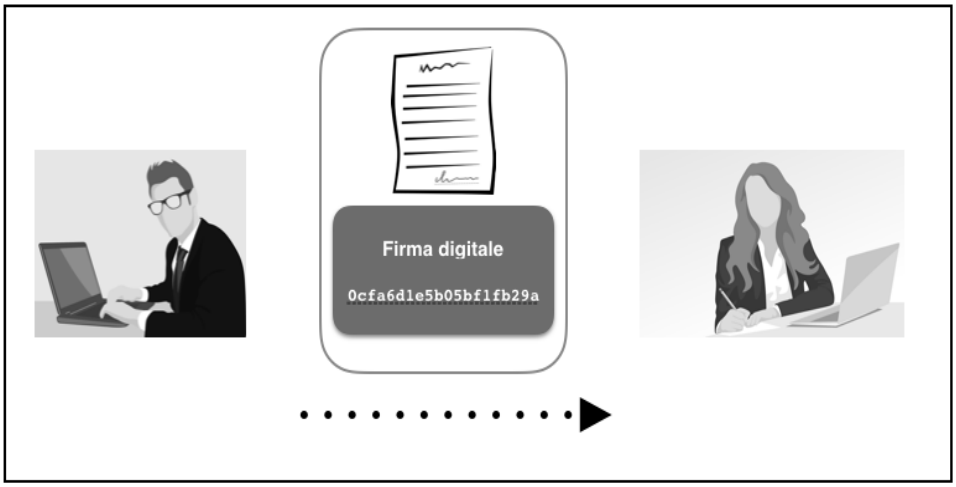
L'utilità dell'uso dell'«impronta» è di tutta evidenza: ci consente di generare la firma digitale senza necessità di criptare l'intero documento.

L'«impronta» rappresenta – poi – il mezzo per ottenerne l'autenticazione da parte di un terzo mantenendo riservato il contenuto del documento che l'ha generata.

La firma digitale, per come abbiamo illustrato, non cripta il documento – che, quindi, rimarrà intellegibile a tutti, vale a dire «in chiaro» – ma ne assicurerà esclusivamente la non alterazione del testo e la provenienza da un soggetto determinato.

Quindi, proseguendo nell'esempio fatto, Andrea, dopo aver applicato al documento la funzione di *hash*, aver ricavato l'impronta ed ottenuto la firma digitale cifrando l'impronta con la propria chiave privata, trasmetterà a Grazia il documento in chiaro con la firma digitale.

Figura 12



La cifratura del testo potrà – invece e come abbiamo già illustrato – essere effettuata a meri fini di segretezza utilizzando la chiave pubblica del destinatario (Grazia), come sopra spiegato.

Arrivati a questo punto sarà più facile la comprensione della definizione di firma digitale data dal D.Lgs. 7 marzo 2005, n. 82 (come modificato dall'art. 1, comma 1, lett. e, D.Lgs. 26 agosto 2016, n. 179) secondo il quale essa è «un particolare tipo di firma qualificata basata 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» (art. 1, lett. s, D.Lgs. 7 marzo 2005, n. 82).