IL CODICE DELL'AMMINISTRAZIONE DIGITALE

D. LGS 82/2005 o Codice dell'Amministrazione Digitale [CAD]: se non diversamente indicato, tutti gli Articoli citati derivano da questo Codice.

In particolare: Art. 1, 20, 21, 23, 24, 25, 26, 27, 29, 30, 32,

1. IL CODICE DELL'AMMINISTRAZIONE DIGITALE
D. LGS 7 marzo 2005 nro 82

Il Codice dell'Amministrazione digitale è un testo unico che riunisce e riordina diverse norme, riorganizzando la materia delle informazioni e dei documenti in formato digitale.

Questo Codice non riguarda, come può sembrare dal nome, solo la pubblica amministrazione: gran parte di queste norme si applicano anche ai privati. Le norme più significative che contiene sono disposizioni sul documento informatico, la firma elettronica e la firma digitale.

Breve storia del Codice dell'Amministrazione digitale

L'Italia è stato il primo paese UE che, nel 1997, si è dotato di una legge su gli argomenti dei documenti in digitale: la Bassanini 1, che aveva come scopo semplificare la comunicazione tra pubbliche amministrazioni e tra pubblica amministrazione e cittadini, evitando le informazioni ridondanti e l'intaso delle poste grazie all'utilizzo del mezzo informatico.

Tra il 1997 e il 2005 sono state emanate diverse norme, che sono poi state riorganizzate nel Codice dell'Amministrazione digitale, il solo che noi vedremo in quanto legge corrente; tutte queste, dalla Bassanini 1 in poi, sono andate a determinare cosa siano i tre concetti di documento informatico, firma elettronica e firma digitale, e stabilire se siano giuridicamente equivalenti a un documento in forma cartacea, a una firma autografa o a una firma autenticata da un notaio.

Due approcci opposti: legiferare per oggetto o per funzione

Il Codice dell'amministrazione digitale riunisce due approcci opposti, due politiche legislative opposte, che si rilevano dal alcune norme tra loro contrastanti.

Nel 1997 il legislatore si è dato una normativa nella quale ha scelto una precisa tipologia di firma, la firma digitale. Egli ha quindi apertamente favorito questo modello, evidentemente perché lo riteneva più sicuro degli altri. Anche la Germania, successivamente, scelse la firma digitale.

Eppure, nonostante questo, quando l'Europa nel 1999 rivolse la sua attenzione a documenti digitali e firme, fece una scelta diversa, ovvero optò per la neutralità tecnologica.

Secondo **il principio della neutralità tecnologica** in una norma non si sceglie una tecnologia specifica ma si permette di utilizzarne di diverse, stabilendo degli obiettivi che la tecnologia dovrà raggiungere. Si tratta quindi di un approccio alternativo, un approccio funzionale: la tecnologia deve garantire alcune cose, specificate dalla norma, e se le garantisce, essa è accettabile.

Lo stesso principio della neutralità tecnologica è al centro dell'attuale dibattito sulla posta elettronica certificata, che è contraria a questo principio.

Legiferare secondo il principio della neutralità tecnologica permette di mantenere libertà di scelta rispetto alle proposte del mercato: in un ventaglio di tecnologie accettabili, ognuno potrà scegliere quella che preferisce, ad esempio ragionando a seconda della spesa che vuole sostenere.

Inoltre, la norma, e questa è un'osservazione molto importante, si adatta meglio al progredire del progresso tecnologico, è più elastico. Una nuova tecnologia migliore delle precedenti può essere immediatamente adottata, dal momento che la legge non vincola a qualcosa di specifico che nel frattempo può essere diventato obsoleto o addirittura non essere più sicuro a fronte dell'evoluzione tecnologica.

Legiferare per oggetto invece che per funzione, tuttavia, rende le norme più chiare e determinate, là dove il principio di neutralità tecnologica delinea norme più generali, indeterminate, addirittura vaghe, e in ultimo difficili da comprendere.

Questa scelta può portare problemi di compatibilità tra le diverse tecnologie che potrebbero potenzialmente essere adottate, e comporta per i giudici la necessità di mantenersi costantemente aggiornati sulle novità tecnologiche. Questo secondo problema tuttavia non è una difficoltà reale in quanto questo è normale per i giudici, e comunque ogni qual volta si trovano a giudicare una

controversia su una materia specifica vengono affiancati da commissioni di consulenti tecnici di ufficio, detti CTU, (esperti informatici nel nostro caso) che gli forniscono perizie tecniche.

L'UE, quindi, sceglie le firme elettroniche nella sua direttiva.
Nel 2002 l'Italia si adegua e inserisce le firme elettroniche nelle sue norme, ma non deroga le leggi precedenti sulla firma digitale. I due approcci convivono quindi nel Codice dell'Amministrazione digitale.

Si può osservare che l'UE tende spesso ad adottare soluzioni che privilegino il libero mercato, cosa che l'Italia non fa con la stessa frequenza. Lo stesso approccio liberale si trova infatti nelle norme sulle autorità di certificazione, dove invece l'Italia aveva scelto un approccio pubblicistico, in cui il certificatore è controllato da un'autorità.

2. IL DOCUMENTO INFORMATICO

Cos'è un documento? Un documento è la rappresentazione di un fatto, indipendentemente dal fatto che la rappresentazione sia costituita, o contenga, parole. Anche una fotografia è un documento, poiché rappresenta in un certo momento una certa realtà. Il documento è anche indipendente dal supporto cartaceo: possono essere documenti una registrazione, o un video, anche senza audio.

Il documento è un concetto amplissimo, del quale nel nostro ordinamento giuridico non esiste una definizione precisa: è considerato un concetto socialmente noto, e condiviso.

La definizione che ne ha dato la dottrina è "cosa che rappresenta un fatto" (Carmel Lutti).

Diverso è il discorso sul documento informatico, che il legislatore del 1997 ha definito nell'Art. 1 lettera p.

Art. 1. Definizioni

1. Ai fini del presente codice si intende per:
   p. documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

Un documento informatico è quindi qualunque rappresentazione, purché digitale, di un fatto. Può trattarsi di un'immagine, una videoripresa, una mail, un documento di Word, una musica, esso rimane anche in questo caso un concetto molto ampio.

Per via della sua natura tecnologica, la firma(elettronica) può sempre accompagnarlo, ma un documento per essere tale non deve essere necessariamente firmato.

Si tratta di un notevole salto culturale. Tutti i documenti digitali possono essere firmati e datati, il che può servire a definire termini, paternità e così via.

Come tutti i documenti, anche quelli digitali sono destinati alla conservazione, si pensi ad esempio alla prova del pagamento di una fattura, e di conseguenza c'è bisogno di un modo per garantirne la leggibilità, la conservabilità e l'integrità nel tempo, sia da un punto di vista pratico che giuridicamente valido.

Il caso della conservazione è rivelatorio sulla diversa essenza del documento informatico rispetto al documento classico. Del secondo è banale fare un'archiviazione che sia valida anche dal punto di vista giuridico, ma non è lo stesso per un documento informatico. I due documento sono diversi nella loro ontologia.

Per i documenti informatici sono state emanate norme ad hoc che riformulano i concetti già consolidati per il documento di classico di firma, valore come prova (efficacia probatoria), conservazione.

3. FIRME E CERTIFICATI

FIRMA ELETTRONICA

Art. 1. Definizioni

1. Ai fini del presente codice si intende per:
   q. firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione identificazione informatica;

Il fine della firma elettronica è consentire di identificare elettronicamente una persona. Esempi di firma elettronica possono essere password, badge, smartcard, o controllo delle impronte digitali..

Secondo l'UNICITRAL vi sono 3 diverse tipologie di firme elettroniche: firme basate su

- qualcosa che si è
  si basano su una caratteristica personale/fisica, ad esempio il riconoscimento della voce, delle impronte digitali, la scansione della retina, le tecnologie biometriche in generale.
- qualcosa che si possiede
  badge, device, smartcard..
- qualcosa che si conosce
  codice pin, password

Il livello di sicurezza di questi sistemi è molto variabile, si pensi a confrontare un pin a 5 cifre come quello del bancomat con una scansione della retina, eppure rientrano nella stessa classificazione dal punto di vista giuridico. Vedremo come la firma elettronica nel nostro ordinamento giuridico non dia grandi garanzie, proprio perché il livello di sicurezza che permette non è fisso, ed è anzi la sua valutazione è soggetta alla discrezionalità del giudice.

FIRMA DIGITALE

Art. 1. Definizioni

1. Ai fini del presente codice si intende per:
   s. firma digitale: un particolare tipo di firma elettronica 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;

Concretamente, si tratta della tecnologia crittografica a chiave asimmetrica, detta anche a chiave pubblica. Una chiave è, in termini semplici, un codice.

Alice e Bob vogliono comunicare, ognuno di essi possiede una coppia di chiavi, di cui una è la cosiddetta chiave pubblica, che entrambi hanno reso noto all'altro, e l'altra è la chiave privata che mantengono segreta.

Le chiavi private devono essere mantenute segrete non solo per buonsenso, ma anche per imposizione di legge.

Se Alice vuole mandare un documento a Bob, può elaborarlo con la sua chiave privata. L'elaborazione è una forma di cifratura, ma permette anche di aggiungere informazioni se lo si desidera.

Bob riceve il documento elaborato da Alice, cifrato con la chiave privata di Alice. Per leggerlo, lo decifrerà con la chiave pubblica di Alice. Questo sistema permette di garantire la provenienza del documento, Bob è certo che il documento derivi da Alice, proviene da Alice, è un documento di

cui Alice è autore. La firma digitale corrisponde quindi a tutti gli effetti alla firma.

Poter identificare la provenienza di un documento significa poter fare un'attribuzione, con la firma si attribuiscono le dichiarazioni del documento al titolare della firma, se ne attesta la provenienza. Essendo la procedura di apporre una firma digitale un'elaborazione sull'intero documento, essa garantisce anche l'integrità del documento stesso.

La firma digitale permette anche comunicazioni private uno a uno, ovvero garantisce la segretezza: è sufficiente che Alice dopo aver cifrato con la propria chiave privata cifri il messaggio una seconda volta con la chiave pubblica di Bob. Solo Bob potrà decifrare il messaggio poiché è il solo a possedere la chiave privata.

In Italia solo le persone fisiche possono possedere chiavi crittografiche.

FIRMA ELETTRONICA QUALIFICATA

Art. 1. Definizioni

1. Ai fini del presente codice si intende per:
   r. firma elettronica qualificata: la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica;

Deriva dal legislatore europeo. Detta i requisiti della firma digitale (crittografia a chiave asimmetrica), pur senza citare la crittografia a chiave asimmetrica in modo esplicito. La procedura che consente la connessione univoca al firmatario è precisamente il sistema a chiave asimmetrica, ciò che gli permette di conservare un controllo esclusivo e collegata ai dati è la chiave privata, e ciò che consente non sono altro che i requisiti di immodificabilità e integrità. Il dispositivo sicuro è il certificato.

CERTIFICATO

Art. 1. Definizioni

1. Ai fini del presente codice si intende per:
   e. certificati elettronici: gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità informatica dei titolari stessi;

La soluzione dell'utilizzo di chiavi crittografiche genera il problema dell'associazione tra le chiavi e la persona fisica. Per risolvere questo problema nascono i certificati elettronici di certificazione, certificati rilasciati da una cosiddetta autorità di certificazione (accreditata/certificata) la quale ha l'onere di accertare l'identità della persona fisica.
Non solo, la responsabilità dei certificatori è molto più elevata: devono gestire anche la revoca e la sospensione dei certificati in modo sicuro e corretto.

In Italia i certificatori possono essere di tre diversi tipi, sempre a causa del duplice approccio della normativa:

- semplici: certificatori senza alcuna autorizzazione ai sensi dell'Art. 26. Non possono rilasciare certificati per la firma digitale, e su di essi non vi è alcun controllo, né è

richiesto alcun requisito per diventare certificatori semplici. Derivano dalla direttiva UE.

- qualificati: ai sensi dell'Art. 27. Devono, per divenire tali, avere diverse caratteristiche, e devono comunicare il loro inizio attività al CNIPA. Derivano dalla direttiva UE, e possono rilasciare certificati per la firma digitale.
- accreditati: devono sottoporsi ad un esame da parte del CNIPA, e devono possedere diverse caratteristiche, tra cui ad esempio un capitale sociale molto alto, paragonabile a quello richiesto per l'inizio dell'attività bancaria. Sono registrati in un albo. Derivano dall'approccio italiano del '97, e possono rilasciare certificati per la firma digitale. La maggioranza dei certificatori sono di questo tipo, per un discorso di concorrenza difensiva. Tra i certificatori accreditati italiani: infocamere, Altalis, Poste, Consiglio nazionale notarile, Consiglio nazionale forense.

4. FORMA DEI DOCUMENTI INFORMATICI

La forma(si intende forma scritta) è un requisito eventuale del contratto. Per molti contratti non è necessaria, in quanto il nostro Codice Civile conserva il principio medioevale della Lex Mercatoria della libertà della forma e permette la conclusione di contratti anche in forma orale o tacita.

Secondo il nostro ordinamento giuridico vi sono tre diverse forme (anticipazioni in *corsivo*):

- forma per la validità del contratto (ad substantiam)

  la forma per l'esistenza del contratto stesso. Alcuni contratti, come ad esempio i contratti per l'acquisto di beni immobili, di costituzione di società, di donazione, richiedono questa forma per essere contratti validi, pena la nullità del contratto stesso ai sensi dell'Art. 1350 del Codice Civile. La donazione è un caso significativo del significato della forma per la validità: la donazione è una volontà rara, e il legislatore vuole la certezza che la volontà sia reale. La forma per la validità è forma per l'espressione di una volontà. Di conseguenza, in questi documenti, è necessaria la firma (oltre alla forma scritta): devono essere scritture private, scritture private autenticate o atti pubblici.

  La forma per la validità si può avere con il documento informatico sul quale sia stata apposta firma digitale o firma elettronica qualificata, secondo l'Art. 20 comma 2, che è il solo a poter essere equivalente a scrittura privata, scrittura privata autenticata, o atto pubblico (dipendentemente da come viene redatto e firmato).

- forma per la prova (ad probatione)

  forma per provare il contratto in giudizio. Ad esempio per i contratti di assicurazione non è richiesta la forma scritta perché il contratto sia valido, ma solo per dimostrare di averlo concluso.

- forma scritta a fini informativi

  talvolta è richiesta la comunicazione di alcune informazioni *per iscritto*. Si tratta di una forma particolare, per la quale non servono firme o notai, la sola richiesta è che le in informazioni vengano veicolate in forma scritta, stampata, in un formato durevole, principalmente allo scopo di poter essere rilette a distanza di tempo. Un esempio di forma scritta a fini informativi è quella prevista dal Codice del Consumo all'Art. 52 e 53.

  Questa forma non è espressione di una volontà, di conseguenza non serve che un documento che sia forma scritta a fini informativi abbia una firma, diversamente da come accade ad esempio per i contratti che richiedono forma scritta per la validità.

  Il documento informatico è idoneo a costituire forma scritta per fini informativi, secondo l'Art. 20 comma 1bis, in modo valutato dal giudice caso per caso.

Il documento informatico si può considerare un documento scritto? Quanto vale? Può valere come forma scritta per la validità, per la prova, o per fini informativi?

Art. 20. Documento informatico

1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dal comma 2.

2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del

> documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.

Questo articolo, al comma 1bis afferma che il documento informatico (privo di firma) è idoneo a essere forma scritta per fini informativi. Tuttavia, la sua idoneità non è fissata a priori, ma viene valutata caso per caso dal giudice, a cui il legislatore rimette la propria volontà. I criteri sui quali il giudice deve basare la sua decisione sono quattro: qualità, sicurezza, integrità e immodificabilità.
Osserviamo che la sicurezza in sé non è solo una caratteristica del documento, bensì di tutto il processo aziendale che deve essere sicuro: sarebbe opportuno che vi venissero utilizzati sistemi di crittografia sicuri come quello a chiave asimmetrica, che vi fosse una descrizione delle scelte aziendali effettuate in materia di sicurezza, dei processi organizzativi. Tutta questa documentazione è molto importante venga prodotta, in quanto un domani potrebbe essere necessario portarla di fronte a un giudice.

Al secondo comma, si afferma che un documento informatico firmato con firma digitale o firma elettronica qualificata vale come forma scritta per la validità: è possibile ad esempio concludere un contratto per l'acquisto di una casa con un contratto in forma digitale se firmato con una di queste due firme. In questo caso la scelta del legislatore è chiara, non lascia discrezionalità al giudice.

Si osserva una lacuna legislativa: il documento informatico con firma elettronica non è oggetto di una norma ad hoc. Di conseguenza, ricade in quanto dispone l'Art. 20 comma 1bis per il documento informatico senza firma.

5. EFFICACIA PROBATORIA DEI DOCUMENTI INFORMATICI

5.1 VALORE PROBATORIO SECONDO L'ART.21

L'efficacia probatoria di un documento, o prova, è la forza che il documento ha in giudizio. Molti documenti possono essere portati in giudizio come prove, e di volta in volta ne verrà valutata la loro attendibilità, ma vediamo tre tipi di documento in particolare, in ordine di efficacia probatoria crescente:

- scrittura privata: è scrittura privata un documento scritto in qualunque forma purché sottoscritto e datato. La scrittura privata fa piena prova delle dichiarazioni (non dei fatti!) fino a che non si disconosce la firma apposta (Art. 2702 CC). Il riconoscimento può essere fatto da chi lo ha firmato, ovviamente, ma può anche essere un riconoscimento legale: se la firma non è riconosciuta da chi l'ha apposta, la controparte può richiedere una perizia calligrafica.
- scrittura privata autenticata: un documento sottoscritto e datato in cui la sottoscrizione è autenticata da un notaio o altro pubblico ufficiale autorizzato. Il notaio accerta le identità dei firmatari (mediante documento di identità), e attesta le identità e che le firme sono state apposte in sua presenza. Per contestare una scrittura privata autenticata, si deve quindi fare una querela di falso nei confronti del notaio per quanto riguarda l'attestazione di autenticità. (Art. 2703 CC)
- atto pubblico: Il ruolo del notaio è differente rispetto a quello che assume nel caso di scrittura privata autenticata. L'atto pubblico proviene dal notaio(o pubblico ufficiale), è del notaio. Il notaio lo redige in prima persona, e in esso dichiara di attestare le volontà delle parti riunite di fronte a lui. L'efficacia probatoria dell'atto pubblico è molto alta: per contestarlo si deve contestare l'intera dichiarazione, con una querela di falso nei confronti del notaio relativamente all'intero documento.

Art. 21. Valore probatorio del documento informatico sottoscritto

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.
2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.
3. L'apposizione ad 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. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

In via interpretativa, il documento informatico con firma elettronica può integrare la scrittura privata. Di nuovo, la valutazione è effettuata caso per caso, l'idoneità del documento è liberamente valutabile dal giudice. C'è grande flessibilità dal punto di vista normativo perché la definizione di firma elettronica è così tanto indeterminata da permettere diversissimi livelli d sicurezza, e il legislatore ha quindi scelto di non ancorarsi al livello più alto o al più basso.

Un vantaggio di questa scelta è che il giudice può valutare caso per caso prendendo in considerazione anche il contesto della firma, e quindi rendendo giustizia al fatto che nella realtà non conta solo la tecnologia per garantire un dato livello di sicurezza, ma anche la condotta comportamentale dei soggetti (ad esempio è chiaro che il sistema informatico più sicuro diventa il

più insicuro se scriviamo le credenziali di accesso su un post-it attaccato sul monitor). Inoltre, una simile norma non costringe ad un aggiornamento normativo continuo rispetto alla tecnologia.

Per contro, nel momento in cui si firma un documento non si può sapere quanto esso varrà in giudizio: se ne avrà una valutazione come prova solo quando servirà come tale. Peraltro, essendo l'Italia uno stato di Civil Law in cui quindi i precedenti non sono vincolanti, non si può far riferimento a sentenze precedenti: ci può essere incertezza sulle decisioni dei giudici, può non esserci omogeneità dei giudizi.

Diverso è per il documento con firma digitale o firma elettronica qualificata: è idoneo a soddisfare il requisito della forma scritta per la validità, corrisponde alla scrittura privata (l'Art. 2702 del Codice Civile è “Efficacia della scrittura privata”).

Nel caso della scrittura privata, essa fa piena prova se la firma è riconosciuta dalla parte contro la quale il documento è prodotto, o se è legalmente riconosciuta (attraverso una perizia calligrafica). Per il documento informatico con firma elettronica qualificata o digitale si cerca di riprodurre la medesima dinamica, anche se l'onere della prova è diverso rispetto alla scrittura privata: in questo caso, la parte che dovrebbe aver firmato può semplicemente dire di non averlo fatto, e poi eventualmente sarà la controparte a chiedere la perizia. Nel caso di documento informatico con firma elettronica qualificata o digitale, al firmatario è posto un onere più gravoso: egli non può limitarsi a dire di non aver firmato, deve dimostrare di non averlo fatto.

Il titolare che vuole disconoscere la propria firma deve dare la prova che il dispositivo sia stato utilizzato da un altro, ad esempio presentando una denuncia di furto. Osserviamo però che, nel caso di furto di un dispositivo di firma elettronica, alla normale denuncia deve seguire la denuncia all'autorità di certificazione, che provvederà alla revoca del certificato. Una motivazione come il furto, è quindi valida solo se ci si trova nel particolare intervallo di tempo tra il furto stesso e la messa in atto della revoca.

Non è una motivazione accettabile, invece, il fatto che qualcun altro fosse a conoscenza delle credenziali per la firma e/o avesse libero accesso al dispositivo, in quanto la legge ne impone la segretezza (e vi sarebbe dunque una negligenza del titolare).

L'efficacia probatoria del documento informatico con firma elettronica qualificata o digitale è quindi maggiore di quella della scrittura privata. Colui che vuole far valere il documento informatico firmato contro qualcuno è favorito, in quanto l'onere della prova non è suo ma della controparte (conseguentemente svantaggiata).

Il certificato qualificato. La norma non è tecnologicamente neutra, infatti ad esempio le tecnologie biometriche non sono per loro natura dotate di certificato, e quindi non sono comprese nella norma anche se molto sicure.

5.2 PROVA E DISCONOSCIMENTO DEI DOCUMENTI INFORMATICI SENZA FIRMA

Art. 23. Copie di atti e documenti informatici

1. All'articolo 2712 del codice civile dopo le parole: «riproduzioni fotografiche» è inserita la seguente: «, informatiche».

[CC] Art. 2712 Riproduzioni meccaniche

Le riproduzioni (Cod. Proc. Civ. 261) fotografiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.

L'Art. 2717 del Codice Civile stabilisce che i documenti sono prove piene in giudizio se colui contro il quale vengono prodotti come prove conferma che questi siano conformi ai fatti. Se egli invece ne disconosce la conformità, perdono valore.

Si tratta di un meccanismo adesivo (il soggetto deve aderire alla rappresentazione dei fatti nei documenti), quasi confessorio. Può sembrare che questa norma conferisca ai documenti generici un'efficacia probatoria particolarmente bassa, ma la nostra giurisprudenza, attraverso la Corte di Cassazione ha ritenuto che:

- il disconoscimento debba essere motivato
- la prova disconosciuta non costituisce più prova piena ma non perde completamente la sua validità, ha comunque valore di *elemento* di prova
- in quanto elemento di prova può contribuire a formare comunque il convincimento del giudice unitamente ad altre prove (non da sola)

L'art. 23 del Codice dell'Amministrazione Digitale stabilisce che la stessa norma è valida anche per i documento informatici.

Per quanto riguarda il disconoscimento motivato osserviamo che la Corte di Cassazione, con la sentenza 9884 dell'11 maggio 2005, ha stabilito che non basta invocare la sua insicurezza per disconoscere una prova di natura informatica. Questa sentenza va in qualche modo contro il senso comune, poiché i sistemi informatici sono insicuri e i documenti(si pensi ai file, ai log..) sono facilmente alterabili e modificabili. Tuttavia, non basta fare un discorso generale su questa insicurezza per disconoscere la prova, bisogna motivare concretamente la propria posizione.

Inoltre un documento informatico disconosciuto(in analogia col documento dell'Art 2717 CC) costituisce ugualmente elemento di prova, e assieme ad esempio, a prove testimoniali, può essere sufficiente a portare a una sentenza (Cassazione, sentenza 11445 del 6 settembre 2001, in merito al licenziamento disciplinare di un dipendente della società Autostrade sostenuto da prove informatiche e testimoniali insieme).

5.3 FIRMA AUTENTICATA

Art. 25. Firma autenticata

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale o altro tipo di firma elettronica qualificata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.
2. L'autenticazione della firma digitale o di altro tipo di firma elettronica qualificata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità del certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.
3. L'apposizione della firma digitale o di altro tipo di firma elettronica qualificata da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.
4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.

La firma digitale o la firma elettronica qualificata sono equivalenti alla scrittura privata, ma la stessa tecnologia può essere utilizzata anche per ottenere un documento equivalente alla scrittura privata autenticata, sempre coinvolgendo un terzo personaggio, un notaio o un pubblico ufficiale autorizzato.

La procedura per apporre una firma autenticata ha un funzionamento analogo alla scrittura privata autenticata: ci si presenta dal notaio(o dal pubblico ufficiale) con un documento di identità e il certificato della firma, e si appone la firma in sua presenza. Il notaio aggiunge al documento una parte in cui attesta che la firma è stata apposta in sua presenza e che lui ha verificato l'identità del firmatario e il suo certificato, e firma questa dichiarazione con la propria firma digitale.

In più, il notaio afferma, accerta, anche che l'atto non sia contrario all'ordinamento giuridico, cosa che non è tenuto a fare nel caso della scrittura privata autenticata.

La firma autenticata esclude l'utilizzo del dispositivo di firma da parte di un altro, e di conseguenza esclude la possibilità di disconoscimento della firma. Ne deriva un'efficacia probatoria maggiore rispetto alla scrittura privata autenticata: la firma è già legalmente riconosciuta.

6. RIEPILOGO SU FORMA E PROVA DEI DOCUMENTI INFORMATICI

Documento informatico	Idoneità a costituire forma scritta	Efficacia probatoria
senza firma (es. un log, una mail)	Valido a integrare la (sola) forma scritta per fini informativi a seconda della valutazione del giudice, che si deve basare sui 4 parametri di qualità, sicurezza, integrità e immodificabilità [Art. 20 comma 1bis]	Art. 25: fa piena prova dei fatti, se non è disconosciuto. La Corte di Cassazione ha sostenuto che se è disconosciuto costituisce elemento di prova invece che prova piena.
con firma elettronica	Come il precedente. Art. 20 comma 1bis.	Art. 21 comma 1 liberamente valutabile dal giudice
con firma elettronica qualificata o firma digitale	Per la validità, Art. 20 comma 2	Art. 21 comma 2, ha l'efficacia probatoria della scrittura privata, dando prova delle dichiarazioni contenute nel documento, se non è disconosciuto. Il disconoscimento deve avvenire con la prova di non utilizzo del dispositivo di firma da parte del titolare.
con firma digitale autenticata	Art. 25 integra la forma scritta per la validità, non c'è una norma che lo dice, ma se ai sensi dell'Art. 20 comma 2 la firma elettronica qualificata o digitale può essere prova per la validità, a maggior ragione lo potrà il documento con firma digitale autenticata. Il funzionario pubblico o notaio verifica: 1. l'identità dei firmatari 2. la validità dei certificati 3. validità dell'atto, che non deve essere contrario alla legge 4. che le firma siano apposte in sua presenza	Stessa efficacia probatoria della scrittura privata autenticata. Fa prova piena, non può essere disconosciuta, può solo essere oggetto di querela di falso. Può anche essere usato come atto pubblico.

7. TRASMISSIONE INFORMATICA DEI DOCUMENTI

Art. 45. Valore giuridico della trasmissione

1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.
2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

I documenti mandati via mail a una pubblica amministrazione sono validi, senza la necessità di far seguire il documento originale con mezzi convenzionali (es. posta).

Il secondo comma di quest'articolo formula la presunzione di conoscenza nel caso di comunicazione tramite mail. La mail si ritiene inviata se spedita al gestore, e consegnata se il gestore la rende accessibile all'indirizzo di posta elettronica del destinatario. Questa presunzione non è completa, bensì semplice: da un fatto certo (ad esempio nel caso della consegna, la disponibilità all'indirizzo corretto) si desume un fatto incerto (che il destinatario l'abbia letta).

Art. 47 (Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni)

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.
2. Ai fini della verifica della provenienza le comunicazioni sono valide se:
   a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
   b) ovvero sono dotate di protocollo informatizzato;
   c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71;
   d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. .
3. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni centrali provvedono a:
   a) istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. , per ciascun registro di protocollo;
   b) utilizzare la posta elettronica per le comunicazioni tra l'amministrazione ed i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

Art. 48 (Posta elettronica certificata)

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. .
2. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. , ed alle relative regole tecniche.

La posta elettronica certificata nasce per le comunicazioni tra/con le pubbliche amministrazioni (ma può essere utilizzata anche in rapporti tra privati) e fornisce le stesse garanzie della raccomandata con ricevuta di ritorno, ovvero che il documento in questione sia stato effettivamente ricevuto dal destinatario.

Questo è garantito dai provider stessi, che certificano l'avvenuto invio e l'avvenuta ricezione.

Possedere una casella di posta elettronica certificata (PEC) era inizialmente una scelta libera, basata sul consenso. Ora non è più così, e la PEC è obbligatoria, oltre che per le pubbliche amministrazioni, per le società di nuova costituzione e per i professionisti iscritti in un albo (a partire da fine novembre 2009). Entro due anni, anche le società costitute prima del novembre 2008 dovranno dotarsi di una casella PEC.

Inoltre, ogni cittadino può richiedere una PEC personale gratuita.

La PEC presenta diversi vantaggi: è economica, è comoda, è veloce. In altre parole, è utile. Tuttavia, pone un grosso problema di consapevolezza informatica e giuridica: un indirizzo PEC individua un domicilio informatico presso il quale le pubbliche amministrazioni possono notificare atti, da alcuni dei quali decorrono dei termini, come ad esempio multe.

Essere titolare di un indirizzo PEC comporta quindi la responsabilità di controllare la casella periodicamente (oltre che di conservare i documenti ricevuti) per prendere visione degli eventuali atti ricevuti.

Inoltre, una volta che si attiva una PEC, anche come privato cittadino, non la si può poi “restituire”.

8. CENNI SULLA CONSERVAZIONE VALIDA SOTTO IL PROFILO GIURIDICO DEL DOCUMENTO INFORMATICO

In breve, deve esserci un responsabile della conservazione che appone la sua firma periodicamente.
E' possibile trasformare il documento in digitale e conservarlo in questa forma, distruggendo la copia cartacea originale.

Art. 44 (Requisiti per la conservazione dei documenti informatici)

1. Il sistema di conservazione dei documenti informatici garantisce:
   a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
   b) l'integrità del documento;
   c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;
   d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in Allegato B a tale decreto.

Dowqx doi2 d