Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea di
Diritto e Tecnologia
a.a. 2022/ 2023

TIME STAMPING: LA VALIDAZIONE TEMPORALE ELETTRONICA DEI DOCUMENTI

RELATRICE:
BEATRICE ZUFFI

STUDENTESSA:
FRANCESCA SANCINETI

SOMMARIO

INTRODUZIONE E SCOPO DELLA TESI

Il processo di digitalizzazione ha inizio con l'avvento dei primi computer intorno agli anni Cinquanta del Novecento, anche se, convenzionalmente lo si colloca nel 2002, poiché a partire da quel momento l'umanità ha cominciato ad immagazzinare una maggiore quantità di informazioni in formato digitale rispetto al passato ([1]).

La digitalizzazione si definisce come il processo di creazione e conversione di dati e processi in formato digitale.

Si tratta di un processo che ha rivoluzionato la nostra vita quotidiana e, in quest'ottica, nemmeno il settore del diritto ha fatto eccezione: la dematerializzazione dei supporti documentali e l'impiego di nuove tecnologie sono stati e sono ancora oggi una sfida per giuristi e avvocati.

Sono questi i presupposti con i quali si vuole dare inizio alla presente tesi di laurea dal titolo "*Time stamping: la validazione temporale elettronica dei documenti".*

Il lavoro, suddiviso in tre capitoli, offre una prospettiva, per quanto possibile, completa sul processo di validazione temporale del documento informatico, considerando il fenomeno non solo dal punto di vista giuridico, ma anche da quello tecnologico.

Tradizionalmente, la sottoscrizione autografa di un documento analogico comporta l'assunzione di paternità da parte di chi vi appone la propria firma, e l'inserimento in esso di data e ora, secondo quanto previsto dal Codice civile, fornisce elementi utili a dimostrare l'esistenza dell'atto in un determinato momento.

Con l'introduzione e il crescente utilizzo del documento elettronico, sono emersi vari quesiti, quali quelli relativi alla paternità dell'atto informatico, alla sua validità e alla sua opponibilità ai terzi.

In particolare, ci si è chiesti in cosa consista il processo di validazione temporale elettronica, quali siano i suoi riconoscimenti a livello normativo e quali tecniche informatiche vengano utilizzate nella prassi in questione.

[1] Per approfondire, si consiglia: HILBERT e LÓPEZ, *The World's Technological capacity to Store, Communicate and Compute Infromation,* in *Science*, 2011, p. 60. In questo articolo gli autori si focalizzano sulla capacità delle tecnologie di gestire le informazioni, in particolare: sulla possibilità di immagazzinare (*storage*), comunicare (*comunication*) e calcolare informazioni (*computation of information*) tra la fine del Novecento e gli inizi del Duemila.

Scopo della tesi sarà, dunque, quello di analizzare la validazione temporale di un documento informatico nella sua interezza, considerandone: la definizione, la funzione, la validità e il procedimento di formazione.

CAPITOLO PRIMO: IL DOCUMENTO TRA TRADIZIONE E INNOVAZIONE

Il documento nel processo civile assume un ruolo fondamentale, perché serve a ricostruire una determinata realtà storica che può essere rilevante per la decisione. Esso rappresenta un fatto, una dichiarazione o un negozio e per tale ragione è utilizzabile nel processo come prova.

La prova è l'oggetto dell'istruzione probatoria, ossia della fase di espletamento dei mezzi di prova, al fine di ricavare le prove necessarie al giudice per decidere la causa.

L'assunzione delle prove è stata nel tempo regolata da due principi contrapposti: da un lato, il principio della prova legale e dall'altro, quello secondo cui la convinzione del giudice si deve formare liberamente ([2]).

Il principio della prova legale prevede che la decisione non sia rimessa al giudice, quanto piuttosto al legislatore che mediante l'atto di legiferazione, estrinsecato con la norma in sé, fissa in astratto il modo in cui il giudice deve cogliere gli elementi di decisione. Sono prove legali l'atto pubblico e la scrittura privata come previsto, rispettivamente, dagli articoli 2699 e 2702 del c.c. (v. atto pubblico e scrittura privata) ([3]).

Nonostante residuino ancora delle prove la cui valutazione è vincolata *ex lege*, il diritto moderno ha, tuttavia, respinto in larga parte il sistema della prova legale a favore del principio del prudente apprezzamento del giudice. Nell'attuale sistema, ampio spazio, è riservato alle prove libere che sono valutate dal giudice secondo il suo prudente apprezzamento: l'esempio classico è quello della testimonianza, la cui attendibilità viene

[2] Ex art. 116 c.p.c.: "*Il giudice deve valutare le prove secondo il suo prudente apprezzamento, salvo che la legge disponga altrimenti.*
Il giudice può desumere argomenti di prova dalle risposte che le parti gli danno a norma dell'articolo seguente, dal loro rifiuto ingiustificato a consentire le ispezioni che egli ha ordinate e, in generale, dal contegno delle parti stesse nel processo."

[3] Il principio della prova legale è un complesso di regole, di derivazione germanica, che disciplinavano in quali casi il giudice dovesse ritenere già provato un fatto. Questo sistema è stato fortemente ripudiato dal diritto moderno, seppure rimangano ancora ad oggi delle rimanenze nel diritto italiano di prova legale, a favore invece del libero convincimento del giudice. Rif. CHIOVENDA, *Principii di diritto processuale civile,* Napoli, 1980, p. 809 ss.

soppesata di volta in volta dall'autorità giurisdizionale, tenendo conto di ogni circostanza utile.

Le regole fondamentali che caratterizzano il processo civile sono: il principio dispositivo e il principio dell'onere della prova ([4]).

Il principio dispositivo, anche noto come principio dell'iniziativa di parte, impone, al giudice, di decidere sulla base dei soli fatti allegati e provati dalle parti, per cui spetta ai litiganti l'iniziativa di introdurre le circostanze rilevanti e darne dimostrazione ([5]). I poteri istruttori che il giudice civile può esercitare d'ufficio sono infatti circoscritti.

L'onere della prova è disciplinato all'art. 2697 c.c.: si tratta di una regola di giudizio e si sostanzia essenzialmente nel porre a carico della parte che propone una domanda l'onere di provare i fatti che ne costituiscono il fondamento e alla parte, che solleva un'eccezione, l'onere di dimostrare il fatto impeditivo, modificativo o estintivo su cui quell'eccezione si sorregge. Ove non risulti assolto l'onere (e il fatto non sia pacifico né notorio e sia stato specificatamente contestato dall'avversario, risultando quindi bisognoso di prova), il giudice riterrà il fatto non esistente e non potrà porlo a base della sua decisione ([6]).

---

[4] Chiaramente l'elenco delle regole fondamentali del processo civile non è completo, per approfondire: CHECCHINI, AMADIO, *Lezioni di diritto privato,* Torino, 2020, p. 67 ss.

[5] Chiovenda considera il principio dispositivo come l'onere di affermare, per la parte, dei fatti in giudizio e lo ricollega all'onere della prova, spiegando che se spesso questi due principi sembrano andare di pari passo, non è sempre così. Ad esempio, nel caso di un fatto notorio si avrà l'onere di affermarlo ma non di provarlo in quanto si considera già certo di per sé. Rif. CHIOVENDA, *Principii di diritto processuale civile,* cit., p. 778.

[6] Tra i fatti non bisognosi di prova si trovano i fatti notori, non contestati e pacifici.
Cfr. DITTRICH, *Le prove nel processo civile e arbitrale*, Milano, 2021, p. 34 dove spiega cosa si intenda per fatto notorio: la conoscenza di quei fatti che costituiscono parte della cultura normale di un determinato gruppo sociale in un preciso periodo di tempo. Anche dalla lettura del co.2 dell'art. 115 c.p.c emerge la codificazione dei c.d. "fatti notori", nella quale si stabilisce che: "*il giudice può tuttavia, senza bisogno di prova, porre a fondamento della decisione le nozioni di fatto che rientrano nella comune esperienza".*
Sono tre le caratteristiche entro le quali si può fare rientrare un fatto in questa categoria. Anzitutto deve trattarsi di un fatto che rientra nell'ambito della comune esperienza. La dottrina si è dibattuta a lungo sull'analisi di questa categoria per questo motivo occorre fare ulteriori precisazioni. La categoria *de qua* non riguarda necessariamente i fatti attuali e positivi ma anche quelli potenziali. Inoltre, con il termine "comune esperienza" ci si riferisce a quei fatti conosciuti da una indistinta comunità di consociati.
Diversi sono i fatti non contestati, ossia quei fatti che la controparte decide di non contestare ovvero di contestare in maniera generica. L'unica contestazione valida deve essere specifica. Nel caso di specie, la controparte potrà allegare anche documenti specifici in modo tale da rendere più dettagliata la contestazione. Per il principio di non contestazione i fatti che la controparte non contesta o sui quali ha mantenuto il silenzio vanno considerati come non contestati. A ribadire questo concetto chiave è anche la Cass. Civ., sez. un., con sentenza n.761 del 23/01/2002, in *DeJure.it*, mediante la quale si spiega che, riconosciuto l'onere per la controparte di contestazione specifica dei fatti allegati dall'attore, la non contestazione si traduce in "*un comportamento univocamente rilevante ai fini della determinazione dell'oggetto del giudizio, con effetti vincolanti per il giudice, che dovrà astenersi da qualsivoglia controllo probatorio del fatto non contestato e dovrà ritenerlo sussistente, proprio per la ragione che l'atteggiamento*

1.1 IL DOCUMENTO COME RAPPRESENTAZIONE E COME PROVA NEL PROCESSO.

Il documento è la rappresentazione di una realtà storica.

Dare al termine rappresentazione una definizione univoca appare molto difficile ([7]), ma è utile ricordare che secondo la concezione carneluttiana la rappresentazione è un surrogato della percezione. Entrambe hanno rilevanza nel mondo esterno seppur in modo diverso.

La percezione deriva dalle attività sensoriali, è proprio attraverso i cinque sensi che si è in grado di percepire e prendere coscienza della realtà.

La rappresentazione in qualche modo si sovrappone alla percezione ma se ne differenzia perché è frutto di un'attività mentale dell'uomo, che chiaramente necessita di estrinsecazione nel mondo esterno per avere rilevanza. Infatti, la rappresentazione dipende dalla volontà e da come l'attività mentale dell'uomo la estrinseca, mentre la percezione prescinde del tutto da questo tipo di attività. I colori, ad esempio, vengono solamente percepiti attraverso i cinque sensi e appaiono in maniera già di per sé definita.

La rappresentazione, invece, richiede l'espletamento di un'attività ulteriore, che implica l'uso di abilità cognitive, e può essere soggettiva o oggettiva.

La rappresentazione soggettiva della realtà è una rappresentazione personale; l'esempio più evidente è quello del testimone ossia di un uomo che attingendo alle sue memorie racconta un avvenimento passato. Si tratta, quindi, di una realtà mediata dalla mente di chi racconta. L'uomo agisce in assenza del fatto da rappresentare ed è solo basandosi sulla

---

difensivo delle parti, valutato alla stregua dell'esposta regola di condotta processuale, espunge il fatto stesso dall'ambito degli accertamenti richiesti".
E ancora, i fatti pacifici sono quelli che la controparte ammette in maniera esplicita oppure quando la parte imposta un sistema difensivo su elementi che di per sé risultano incompatibili con il disconoscimento.

[7] In primo luogo, ci si è chiesti se la rappresentazione fosse solamente l'elemento intrinseco, la proprietà statica del documento dove semplicemente la rappresentazione è il mezzo attraverso il quale si conosce qualcos'altro; oppure se fosse il processo dinamico utilizzato dal documentatore per formare il documento stesso. Dare una definizione univoca al concetto di rappresentazione appare fin da subito molto complicato, anche guardando al significato più comune del termine come quello presente nel *Vocabolario della lingua italiana Treccani: "attività e operazione di rappresentare con figure, segni e simboli sensibili, o con processi vari, anche non materiali, oggetti o aspetti della realtà, fatti e valori astratti, e quanto viene così rappresentato"* (Rif. https://www.treccani.it/vocabolario/rappresentazione/). Per questo motivo, il presupposto *aut aut* nei confronti di una rappresentazione come elemento intrinseco del documento oppure come processo dinamico ossia quella attività che si svolge nella mente del documentatore, deve essere sostituito con quello più semplice di *et et*. Rif. NAVONE, *Instrumentum digitale. Teoria e disciplina del documento informatico,* Milano, 2012, p.18

propria memoria e sulle proprie reminiscenze che è in grado di riportare un fatto già avvenuto nel passato.

Diversamente, la rappresentazione oggettiva corrisponde ad una rappresentazione reale di un fatto, ne è un esempio il documento. In questo caso l'uomo agisce in presenza del fatto per produrre un apparato, proprio il documento, che ha la funzione di conservare, in maniera permanente, il fatto rappresentativo.

Ne discende che, l'unica accezione di rappresentazione utile allo scopo della presente disamina è quella relativa ad una rappresentazione oggettiva, in cui il documento assurge a contenitore di quella rappresentazione di una data realtà.

Il documento è una *res* mobile in grado di veicolare la conoscenza della rappresentazione di un fatto, come confermato anche dall'etimologia del termine, che proviene dal latino *documentum,* derivato di *docēre* ossia "insegnare, dimostrare".

Allo studio del documento come prova ha contribuito in maniera decisiva un celeberrimo avvocato e giurista italiano del Novecento, Francesco Carnelutti.

Il documento è la rappresentazione di un fatto, ma -si è sostenuto- esso potrebbe essere definito anche come l'oggetto contenente una manifestazione del pensiero ossia come il frutto di quei processi sensibili diretti a determinare un fatto ([8]).

A quest'ultima descrizione Carnelutti muove due critiche, considerando il concetto di manifestazione del pensiero, da un lato, non sufficiente e dall'altro nemmeno necessario.

Per quanto riguarda il primo versante, egli si avvale dell'esempio di una cartolina contenente la sola scritta "cordiali saluti". Quest'ultima è chiaramente una manifestazione di pensiero: si tratta di un saluto formale diretto ad un determinato soggetto, ma – a suo avviso- non costituisce un documento.

Infatti, la mera scritta "cordiali saluti" integra certamente una manifestazione del pensiero che però in quanto tale non è in grado di dimostrare nulla. Ecco perché alla definizione di documento non è sufficiente l'associazione alla manifestazione del pensiero.

[8] Per CARNELUTTI, *La prova Civile, parte generale, il concetto giudico della prova*, Milano, 1992, p.140 "*Il documento non è soltanto una cosa, ma una cosa rappresentativa, cioè capace di rappresentare un fatto".*
Cfr. DITTRICH, *Le prove nel processo civile e arbitrale*, cit., p. 162 il quale mette in luce l'attitudine rappresentativa del documento ossia l'idoneità di ricreare nella mente di chi ossera un fatto. Nella visione processuale, il documento è rilevante solo qualora fosse in grado di provare un fatto utile per la decisione.

Qualora invece, nella cartolina ci fosse stata anche la firma di chi manda i saluti allora in questo caso non saremmo solo nella manifestazione di un fatto ma in una vera e propria rappresentazione di un fatto. Ecco, quindi, che ciò che risulta essenziale nella definizione di documento è la rappresentazione di un fatto e non tanto la mera manifestazione del pensiero che da sola non è in grado di dimostrare nulla ([9]).

Relativamente al secondo profilo, lo studioso dimostra la non indispensabilità della manifestazione del pensiero nella definizione di documento, facendo riferimento a due strumenti all'epoca frequentemente utilizzati come prove: la fotografia e la fonografia. I fatti fotografati o registrati sono fissati su un supporto (visivo o audio) mediante lo strumento stesso e non per mezzo della rielaborazione della mente umana.

Per i motivi sopra elencati, emerge che la definizione di documento dovrebbe focalizzarsi esclusivamente sul concetto essenziale di "rappresentazione di un fatto", senza che si avverte l'esigenza di integrare nella nozione l'elemento della manifestazione del pensiero.

Questa posizione si considera tutt'ora valida, e si ricorda, a mero titolo dimostrativo, che è lo stesso Codice dell'Amministrazione Digitale a disciplinare il documento come la *"rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".*

Fino a questo punto si è cercato di delineare il concetto di documento focalizzandosi sulla sua capacità rappresentativa. Ora si tratta di stabilire che tipo di prova è quella documentale e di enuclearne i tratti salienti.

Come si è visto, il documento ha carattere permanente nella sua capacità di dimostrare fatti, per cui è indubbio che esso possa essere utilizzato nel processo al fine di fornire la prova delle circostanze che si reputano rilevanti.

Perciò la prova è il mezzo che serve al giudice per valutare la veridicità o la falsità dei fatti in sede processuale. Ne deriva chiaramente la funzione dimostrativa della prova, dal latino *demonstrare*, derivato di *monstrare* ossia 'mostrare', ciò che si mostra all'interno del processo è l'evidenza del fatto ([10]).

---

[9] V. *amplius* CARNELUTTI, *La prova Civile, parte generale, il concetto giudico della prova*, cit., pp. 140-145.

[10] Per approfondire: CAVALLONE, *Forme del procedimento e funzione della prova (ottant'anni dopo Chiovenda)*, in *Rivista di diritto processuale*, 2006, p.417.
In base a quanto visto fino ad ora, l'unica funzione della prova è quella dimostrativa poiché dal momento della decisione del giudice si dovrà essere in grado di ripercorrere l'iter logico compiuto dagli egli stesso.

La prova, quindi, è la fonte di conoscenza dalla quale il giudice valuta la veridicità o meno dei fatti portati in giudizio dalle parti. È da questa valutazione da parte del giudice che deriva la decisione della controversia, per cui nella motivazione deve infatti emergere in maniera logica e razionale il ragionamento fatto dal giudice.

La logica qui in esame è una logica di tipo deduttivo-dimostrativo, nella quale il presupposto è necessariamente un'argomentazione deduttiva: vale a dire che il nesso di consequenzialità tra le premesse di un fatto e le conclusioni stesse è certo. La necessità che il discorso sia razionale deriva dall'esigenza che la sentenza sia controllabile anche dalle parti ([11]).

Le prove all'interno del processo possono essere classificate in vario modo.

La prova, anzitutto, può essere costituenda o precostituita. Nel primo caso, la prova costituenda è quella si crea all'interno del processo mediante l'attività di assunzione dei mezzi di prova. Per esempio, la testimonianza è una prova costituenda in quanto formatasi dinanzi al giudice.

Perciò la funzione retorico-argomentativa non può trovare alcun appiglio poiché, in questo caso, la decisione del giudice sarebbe lasciata alla persuasione e alla sfera soggettiva che in quanto tale non ricostruibile perché non basata su fatti o dimostrazioni oggettive. In altre parole, affinché la decisione del giudice sia ricostruibile, questa deve essere basata su un procedimento razionale; quindi, un procedimento basato sulla persuasione non sarà adeguato. Per di più ciò che si evidenzia è la funzione prettamente giustificativa della scelta razionale del giudice. Tuttavia, si identifica la possibilità per il giudice di fondare la propria decisione sulle massime d'esperienza, a questo fine Taruffo le identifica come "*nozioni comunemente accettate dall'ambiente sociale e culturale nel quale la decisione viene formulata"* e non deve trattarsi di nozioni che siano state falsificate o contraddette da conoscenze scientifiche. Anche in questo caso, qualora il giudice scegliesse basandosi su una massima d'esperienza, si potrà comprendere come egli sia giunto alla decisione considerando i criteri oggettivi. Per tutto quello detto in nota il rif. è CARRATTA, *Funzione dimostrativa della prova (verità del fatto nel processo e sistema probatorio),* in Rivista di diritto processuale, 2001, p.73.

[11] Contrapposta all'argomentazione deduttiva, il cui nesso di consequenzialità tra premesse e conclusioni è certo, si trova l'argomentazione induttiva. In questo caso il nesso di consequenzialità non è più certo ma è solo probabile.

Con riguardo alla razionalità che deve caratterizzare il discorso del giudice, sono diversi i requisiti che si richiedono: linguisticamente corretto; completo nel senso che non dovrò essere trascurato alcun elemento di conoscenza che se mancante non renderebbe comprensivo l'iter logico compiuto dal giudice; rappresentativo e attendibile (in merito alle fonti utilizzate) e ancora plausibile; coerente e congruo. Questi sono tutti gli elementi che dovrebbero caratterizzare la razionalità utilizzata dal giudice al fine di compiere una decisione quanto più attendibile e certa possibile e anche affinché il tutto sia comprensibile dalle parti. Rif. POLI, *Logica e razionalità nella ricostruzione giudiziale dei fatti*, in *Rivista di diritto processuale*, 2020, p. 515.

Inoltre, sempre nell'ottica della logica che il giudice deve usare, si individua anche il principio del "più probabile che non". Si tratta di un principio di diritto per il quale il giudice, nel caso in cui vi siano più concause, dovrà considerare solamente quella che ha un grado di conferma logica superiore vale a dire quella che è la più probabile. (ex multis, la più recente, Cass. Civ, sez. III, con sentenza n.10978 del 26/04/2023).

Invece, la prova precostituita si forma prima e al di fuori del processo, come nel caso dell'atto pubblico che, durante il processo, dovrà semplicemente essere esibito.

Poi, le prove si possono classificare in dirette ovvero indirette, ciò che le differenzia non è tanto la loro funzione quanto piuttosto la loro struttura.

La prova diretta o immediata, si definisce tale in quanto l'attività del giudice è limitata alla sola percezione del fatto da provare ossia dell'oggetto di prova. Strumenti di questa attività sono i suoi sensi: ad esempio, fonte di percezione della prova è l'occhio rispetto ad un documento ovvero l'udito in riferimento alla testimonianza quando il giudice dovesse ascoltare le affermazioni del teste. Rientrano in questa categoria le prove documentali.

La struttura della prova indiretta è più articolata: tra il fatto da provare e il giudice vi è un passaggio intermedio. Non a caso questa prova si definisce mediata. Il mezzo di prova in esame non è più la percezione del giudice, bensì le sue cognizioni ossia il suo sapere: è infatti necessario che il giudice compia un'attività di deduzione di un fatto esterno per giungere all'oggetto di prova. Detto ciò, anche l'attività di percezione del giudice è limitata, in quanto, non è in grado di vedere o udire tutto e il suo sapere è limitato. Per questo motivo, nel caso in cui sia richiesto un elevato sapere tecnico in una determinata materia il giudice può avvalersi della figura dei periti.

Infine, le prove possono essere atipiche ovvero tipiche.

Le prove atipiche è chiaro che queste non siano citate né nel codice civile che nel codice di rito e per questo motivo vi è un dibattito aperto circa quali prove possono rientrare nella categoria *de qua*. È pacifico che possano formare questa categoria i documenti provenienti da terzi come perizie stragiudiziali, consulenze tecniche, o ancora dichiarazioni rese da soggetti che potrebbero essere chiamati a testimoniare ([12]).

[12] In merio all'elenco dei documenti resi da terzi che possono rientrare nella categoria delle prove atipiche è necessario chiarire che si tratta di una grande varietà di documenti e che il loro risultato deriva da un lungo dibattito dottrinale dove semplicemente vi era chi credeva che le uniche prove che potevano entrare a far parte del processo erano quelle tipiche; e dall'altra coloro che consideravano che le prove atipiche dovessero avere minor forza provatoria come quella riconosciuta agli argomenti di prova (ex. art. 116. Co.2 c.p.c.).
Tuttavia, si ritiene necessario citare qui, a titolo esemplificativo, alcune tipologie di prova atipiche come la perizia stragiudiziale ossia la relazione tecnica proveniente da un esperto in una determinata materia e richiesta da una delle parti litiganti. O ancora le prove raccolte o le sentenze rese in altri giudizi rientrano in questa categoria. DITTIRCH, *Le prove nel processo civile e arbitrale,* cit.*,* p.13 e ss.

Quanto alle prove tipiche, ossia quelle citate nel Codice civile e nel Codice di procedura civile si suddividono a loro volta in due macrocategorie: le prove orali e le prove scritte. Le prove orali disciplinate dal Codice civile, sono, appunto, delle prove rese oralmente da soggetti estranei al contenzioso è il caso della testimonianza, alla quale è dedicato l'intero Capo III del Libro VI- delle tutele dei diritti del codice civile; o della confessione, Capo V dello stesso libro. Ancora tra le prove tipiche ci sono le c.d. prove documentali.

Queste verranno analizzate nel prossimo paragrafo ma preme riassumere che si tratta di prove precostituite (formatesi fuori e prima del processo) che faranno ingresso in quest'ultimo attraverso la produzione di documenti ad opera delle parti.

1.2 LE PROVE DOCUMENTALI

A questo punto si ritiene necessario approfondire, qui di seguito, le principali prove documentali regolamentate dal Codice civile (in seguito c.c.).

La prova documentale corrisponde alla rappresentazione di un fatto incorporato su una base materiale in modalità analogica o digitale. Tuttavia, anche delle cose, che in sé non avrebbero funzione rappresentativa, possono servire a provare dei fatti in giudizio. Si tratta del c.d. *sample* (ad es. ad un mattone o ad un campione di calcestruzzo nel caso di controversie su vizi di costruzione di immobili) o di altra cosa che di per sé non è un campione, ma fornisce la dimostrazione di un determinato fatto: si pensi alla produzione- spontanea o disposta con ordine di ispezione- di un bene danneggiato in una causa di risarcimento del danno).

Appare poi utile specificare un'ulteriore differenza all'interno della categoria dei documenti: quelli dichiarativi e quelle narrativi.

I documenti dichiarativi di regola si formano al fine di produrre degli effetti giuridici sostanziali. Ad esempio, mediante la stipulazione di un contratto nascono dei diritti e delle obbligazioni in capo alle parti che lo hanno sottoscritto.

Diversa è invece la situazione nel caso di un documento narrativo, come nel caso di una dichiarazione testimoniale, dove il fine è unicamente quello di descrivere fatti o eventi (ex art. 257-*bis* c.p.c.).

Un'ultima premessa che si ritiene essenziale spiegare riguarda la differenza tra la forma *ad substantiam* e *ad probationem*.

Il termine *ad substantiam* deriva dal latino e significa "ai fini della sostanza", vale a dire che per alcuni atti giuridici l'unica forma richiesta affinché possano essere considerati validi ed efficaci è quella scritta ([13]).

Anche il termine *ad probationem* deriva dal latino e significa "ai fini della prova", quindi rileva soprattutto nel contesto processuale, in quanto la forma scritta è stabilita per la prova in giudizio di un determinato atto giuridico (ad es. il contratto di assicurazione o di transazione può essere dimostrato solo attraverso la produzione del documento che lo rappresenta, al contrario degli altri contratti, per la cui prova è ammessa la testimonianza nei limiti di cui agli artt. 2721 ss c.c.).

1.2.1 ATTO PUBBLICO

L'articolo 2699 c.c. regolamenta la più importante tra le prove documentali ossia l'atto pubblico ([14]).
Si tratta di un atto redatto con particolari formalità da un notaio o da un pubblico ufficiale a ciò autorizzato, in quanto soggetti investiti della funzione di certificare la verità dei fatti e delle dichiarazioni che hanno luogo dinnanzi a loro.

Dal momento che il legislatore ha affidato ad un soggetto accreditato la funzione di rilevanza pubblicistica di attestare una determinata vicenda, questa documentazione farà piena prova della provenienza dell'atto da chi lo ha formato e delle circostanze e delle dichiarazioni avvenute in sua presenza ai sensi dell'art. 2700 c.c. ([15]) fino a querela di falso.

Il documento in questione, come anche la scrittura privata che analizzeremo nel seguito, gode dell'efficacia di prova legale, in quanto vincola il giudice a ritenere dimostrata la provenienza dell'atto e veri il fatto o la dichiarazione attestai, a meno che non sia appunto provato che si tratti di un falso.

Il reato di falso può essere materiale ovvero ideologico:

---

[13] Sul tema si sofferma brevemente anche Delfini dove spiega che la tecnica tradizionalmente intesa per la forma scritta subirà delle evoluzioni in relazione alle tecniche multimediali ad oggi utilizzate. Rif. DELFINI e FINOCCHIARO, *Diritto dell'informatica,* Milano, 2014, p. 275.

[14] *"L'atto pubblico è il documento redatto, con le richieste formalità, da un notaio o da altro pubblico ufficiale autorizzato ad attribuirgli pubblica fede nel luogo dove l'atto è format."*

[15] *"L'atto pubblico fa piena prova, fino a querela di falso, della provenienza del documento dal pubblico ufficiale che lo ha formato, nonché delle dichiarazioni delle parti e degli altri fatti che il pubblico ufficiale attesta avvenuti in sua presenza o da lui compiuti".*

- il primo riguarda l'aspetto estrinseco del documento ossia l'autenticità dell'atto; perciò, il documento potrebbe essere non autentico (non rogato dal notaio che risulta dallo stesso) o potrebbe essere stato manipolato dopo la sua stesura;
- il secondo concerne, invece, la genuinità delle dichiarazioni rese e alla loro corrispondenza alla verità.

Nel caso in cui il soggetto contro il quale l'atto è prodotto, voglia contestare l'autenticità dei fatti compiuti o delle dichiarazioni rese davanti al notaio o al pubblico ufficiale autorizzato, ossia che è stato posto in essere un falso materiale, dovrà farlo mediante querela di falso, come previsto dall'art. 221 del codice di procedura civile ([16]).

La querela di falso è l'unico mezzo che rende vulnerabile l'efficacia probatoria del documento in questione: scopo di questo strumento è, infatti, la rimozione del valore del documento e la contestuale eliminazione di qualsiasi effetto ad essa attribuito.

Invece, qualora il documento contenga affermazioni non veritiere (quelle ad es. rese dalle parti in presenza del notaio) ossia si abbiano dubbi circa l'intrinseco, queste potranno essere provate mediante i normali mezzi di prova ([17]).

Si ricorda, al fine della presente disamina, che la querela di falso qui citata rileva in sede civile, infatti, l'oggetto di falsità consiste nell'accertare se un documento debba o meno essere privato della sua efficacia probatoria privilegiata quando falso.

1.2.2 SCRITTURA PRIVATA

Anche la scrittura privata rientra nell'alveo delle prove documentali.

La scrittura privata consiste in un documento scritto e sottoscritto dall'autore delle dichiarazioni contenute in esso. Gli elementi essenziali di questo documento sono tre: la

---

[16] *"La querela di falso può proporsi tanto in via principale quanto in corso di causa in qualunque stato e grado di giudizio, finché la verità del documento non sia stata accertata con sentenza passata in giudicato. La querela deve contenere, a pena di nullità, l'indicazione degli elementi e delle prove della falsità, e deve essere proposta personalmente dalla parte oppure a mezzo di procuratore speciale, con atto di citazione o con dichiarazione da unirsi al verbale d'udienza.*
È obbligatorio l'intervento nel processo del pubblico ministero."

[17] Quanto appena spiegato in merito all'efficacia probatoria dell'atto pubblico e alla querela di falso è ribadito anche da una recente sentenza della Cass. Civ., sez. VI, sentenza n.20214 del 25/07/2019 in *DeJure.it* che prevede che *"L'efficacia probatoria dell'atto pubblico, nella parte in cui fa fede fino a querela di falso, è limitata agli elementi estrinseci dell'atto, indicati all'art. 2700 c.c., e non si estende al contenuto intrinseco del medesimo, che può anche non essere veritiero. E' pertanto ammessa qualsiasi prova contraria, nei limiti consentiti dalla legge, in ordine alla veridicità e all'esattezza delle dichiarazioni rese nel menzionato atto dalle parti."* (anche Cass. Civ., sez. II, sentenza n.22903 del 29/09/2017; Cass. Civ., sez. III, sentenza n. 25213 del 27/11/2014; Cass. civ., sez. I, sentenza n.11012 del 9/05/2013).

cosa ossia ciò che è destinato a contenere i segni grafici che formano la scrittura, il testo stesso e la sottoscrizione da parte di colui che se ne assume la paternità.

Ad oggi, a livello codicistico non si trova ancora una definizione di scrittura privata, bensì solamente la previsione dei suoi effetti probatori: in base all'articolo 2702 ([18]) essa fa piena prova, fino a querela di falso, della provenienza da chi l'ha firmata, non invece della veridicità delle dichiarazioni contenute nel documento, quando la sottoscrizione è riconosciuta da chi l'ha apposta ovvero è legalmente considerata come riconosciuta (in quanto autenticata da notaio o da altro pubblico ufficiale competente ovvero non disconosciuta nei modi previsti dall'art. 215 c.p.c.) ([19]).

La condizione necessaria affinché la scrittura privata goda dell'efficacia probatoria dell'art. 2702 è che la sottoscrizione sia autentica. Questa si considera tale quando espressamente riconosciuta in giudizio dal soggetto che ha sottoscritto l'atto oppure dalla legge.

La legge disciplina il riconoscimento tacito all'art. 215 c.p.c. e prevede due casi:

- nel caso di contumacia dell'autore del documento o del suo avente causa dove la contumacia è la situazione che si verifica quando la controparte non si costituisce in giudizio;
- e in caso di disconoscimento non tempestivo vale a dire quando la scrittura non è stata disconosciuta entro la prima udienza utile.

Nel caso in cui il soggetto non riconoscesse la firma autografa in calce alla scrittura avrà l'onere di esplicito disconoscimento della stessa ([20]). Nel caso in cui fossero gli eredi o gli aventi causa a disconoscere l'atto, questi dovranno compiere una semplice dichiarazione di non conoscenza dell'atto sottoscritto.

---

[18] *"La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta".*

[19] Il riconoscimento può essere espresso (Cass. Civ,, sez. III, sentenza n. 22460 del 27/09/2017; Cass, Civ., sez. I, sentenza n.21744 del 17/11/2004) oppure anche tacito in base a quanto previsto all'art.215 c.p.c. Il riconoscimento tacito può avvenire in caso di autore contumace del documento o del suo avente case ovvero nel caso in cui non avvenga in modo tempestivo ossia nella prima udienza utile o successiva alla produzione del documento.

[20] Il disconoscimento deve avvenire ai sensi dell'art. 214 c.p.c. e in base a quanto previsto dalla norma tramite questo processo si vuole *negare formalmente la propria scrittura o sottoscrizione;* è chiaro che qualora questo non avvenisse in maniera tempestiva allora la scrittura privata si considererà riconosciuta.

Tuttavia, preme ricordare che in caso di disconoscimento la parte che intende avvalersi della scrittura ha l'onere di proporre l'istanza di verificazione. Il fine principale dell'istanza di verificazione è verificare la provenienza della sottoscrizione e in un qualche modo quello di far acquisire alla scrittura privata l'efficacia probatoria di cui godeva prima dell'avvenuto disconoscimento ([21]).

La data nella scrittura privata in esame può essere opposta ai terzi solo quando è certa, come stabilito dall'art. 2704 c.c. ([22]).

Anche la scrittura privata non autenticata ma a cui è stata apposta una data, può essere opponibile ai terzi come previsto dalla norma in esame, dal giorno:

- in cui la scrittura è stata registrata presso qualsiasi ufficio territoriale dell'Agenzia delle Entrate; oppure
- della morte o sopravvenuta impossibilità fisica da parte del soggetto o dei soggetti che hanno sottoscritto l'atto; o
- in cui il contenuto della scrittura privata è stata riprodotto in atti pubblici; oppure
- in cui si verifica un altro fatto idoneo a stabilire in *modo egualmente certo* la preesistenza del documento.

In primo luogo, l'articolo in questione istituisce la distinzione tra le parti e i terzi: sono considerate parti, oltre a chi ha sottoscritto il documento, i soggetti che hanno un rapporto sostanziale con il documentato, mentre i terzi sono coloro che sono suscettibili di pregiudizio derivante dall'atto stesso.

La data nella scrittura privata non è essenziale. Infatti, la sua mancanza non ne impedisce gli effetti probatori. Ciò nonostante, si ricorda che questa regola trova delle eccezioni: in

[21] Per l'istanza di verificazione ex art. 216 c.p.c. prevede che "*La parte che intende valersi della scrittura disconosciuta deve chiederne la verificazione, proponendo i mezzi di prova che ritiene utili e producendo o indicando le scritture che possono servire di comparazione.*
L'istanza per la verificazione può anche proporsi in via principale con citazione, quando la parte dimostra di avervi ; ma se il convenuto riconosce la scrittura le spese sono poste a carico dell'attore".
Se si volesse approfondire l'argomento DITTRICH, *Le prove nel processo civile e arbitrale*, cit., p. 199 ss.
[22] *"La data della scrittura privata della quale non è autenticata la sottoscrizione non è certa e computabile riguardo ai terzi, se non dal giorno in cui la scrittura è stata registrata o dal giorno della morte o della sopravvenuta impossibilità fisica di colui o di uno di coloro che l'hanno sottoscritta o dal giorno in cui il contenuto della scrittura è riprodotto in atti pubblici o, infine, dal giorno in cui si verifica un altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento.*
La data della scrittura privata che contiene dichiarazioni unilaterali non destinate a persona determinata può essere accertata con qualsiasi mezzo di prova.
Per l'accertamento della data nelle quietanze il giudice, tenuto conto delle circostanze, può ammettere qualsiasi mezzo di prova."

determinati casi la legge prevede esplicitamente la data come requisito essenziale come nel caso del testamento olografo ([23]).

In proposito la Cassazione ha precisato come la certezza della data in una scrittura privata non autenticata possa essere garantita, anche qualora manchino le situazioni tipiche previste dalla norma in questione; l'importante è che vi siano altri fatti idonei a garantire in modo sicuro la data al documento in esame ([24]): come esplicita chiaramente la parte finale dell'art.2704 c.c., il legislatore non ha inteso fornire un'elencazione tassativa dei fatti idonei a garantire data certa ad una scrittura privata non autenticata; sarà, perciò, lasciata al giudice di merito la valutazione delle circostanze addotte dalla parte caso per caso ([25]).

1.2.3 RIPRODUZIONI MECCANICHE

Le riproduzioni meccaniche, contemplate all'articolo 2712 c.c., ossia fatti o cose come riproduzioni informatiche o fotografiche, hanno valore di prova legale se non vi è un disconoscimento della parte contro la quale sono prodotte ([26]).

Ancora una volta si ritiene utile specificare che l'elenco in essa contenuto in merito alle tecniche di riproduzione non è tassativo. Pertanto, la clausola contenuta nella norma in esame ha portata generale e sarà applicabile ad ogni possibile tecnica di riproduzione, comprese quelle sconosciute al momento dell'entrata in vigore della norma (si noti che la disposizione è stata integrata dall'art.23, ora art. 23- quater, del Codice

---

[23] Rif. CIAN, TRABUCCHI, *Commentario breve al Codice civile*, Milano, 15 ed., 2022, sub. Art. 2704 c.c., pag. 3593-3596;

[24] Cass. Civ., sez. III, con sentenza n.13943 del 3 agosto 2012, in *DeJure.it,* prevede che: *"In tema di data della scrittura privata, qualora manchino le situazioni tipiche di certezza contemplate dall'art. 2704, comma 1, c.c., ai fini dell'opponibilità della data ai terzi è necessario che sia dedotto e dimostrato un fatto idoneo a stabilire in modo ugualmente certo l'anteriorità della formazione del documento. Ne consegue che tale dimostrazione può anche avvalersi di prove per testimoni o presunzioni, ma solo a condizione che esse evidenzino un fatto munito della specificata attitudine, non anche quando tali prove siano rivolte, in via indiziaria e induttiva, a provocare un giudizio di mera verosimiglianza della data apposta sul documento."*
Rif. TARASCHI, *Opponibilità ai terzi della data di una scrittura privata non autenticata*, in *IUS Processo civile*, 2021.

[25] Risulta pacifico che l'elenco presente all'art. 2704 non sia tassativo e che sono stati ritenuti idonei ad assicurare data certa ad una scrittura privata non autenticata anche, per esempio, la morta o la sopravvenuta impossibilità fisica di colui o di uno di coloro che l'hanno sottoscritta. (ancora CIAN, TRABUCCHI, *Commentario breve al codice civile*, cit., sub. Art. 2704 c.c., pag. 3594-3595).

[26] *¨Le riproduzioni fotografiche, informatiche 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".*

dell'Amministrazione Digitale di cui al d.lgs. n.82 del 2005, proprio al fine di includervi pure le riproduzioni informatiche).

L'efficacia probatoria delle riproduzioni è controversa. Sembrerebbe trattarsi un'ipotesi di prova legale rispetto alle riproduzioni meccaniche ed informatiche, ma solamente nel caso in cui queste non vengano disconosciute dalla parte contro la quale sono state prodotte. Nel caso in cui avvenga un disconoscimento allora le riproduzioni meccaniche saranno pur sempre liberamente valutabili ([27]).

Si ricorda che il disconoscimento da parte di colui contro il quale la riproduzione meccanica è prodotta deve rispettare determinati requisiti, ed è diverso da quello della scrittura privata che, invece, deve avvenire ai sensi degli art. 214 e 215 c.p.c ([28]).

1.3 IL DOCUMENTO ANALOGICO

1.3.1 TEORIA DEL DOCUMENTO

Il documento analogico, ossia quello tradizionalmente vergato o sottoscritto a mano, si caratterizza per due elementi fondamentali: da un lato, vi è l'imputabilità del documento al suo autore, assicurata come vedremo dalla sottoscrizione ossia dall'atto di apporre il proprio nome e cognome alla fine del documento; dall'altro, vi è l'immodificabilità dello stesso.

Quanto a quest'ultimo elemento preme sottolineare che si tratta di un concetto relativo. È relativo in quanto l'immodificabilità è strettamente collegata al fatto che, qualora vi fosse una manomissione del documento, questa sarebbe evidente. Tuttavia, vi sono casi in cui il documento, anche dopo la sottoscrizione della firma, può essere modificato come nel

[27] Per approfondire il tema degli effetti giuridici delle riproduzioni meccaniche: PATTI, *Commentario del codice civile, Libro Sesto- della tutela dei diritti,* Zanichelli, 2015, p. 482 e ss.

[28] Il disconoscimento delle riproduzioni meccaniche è innanzitutto diverso da quello previsto per la scrittura privata e perciò non soggetto agli art. 214 e 215 c.c. (Cass. Civ., sez. lav., sentenza n. 3122 del 17/02/2015 e Cass. Civ., sez. III, sentenza n. 1033 del 17/01/2013). In quanto alle modalità è emerso che solo un disconoscimento *chiaro, circostanziato e esplicito* è in grado di far perdere alle riproduzioni meccaniche la loro qualità di prova, con la possibilità di concretizzarsi anche mediante l'allegazione di elementi in grado di attestare la non corrispondenza tra realtà fattuale e realtà riprodotta (*ex multis* Cass. Civ., sez. VI, sentenza n.12794 del 13/05/2021, Cass. Civ. sez. II, sentenza n. 1220 del 17/01/2019.). Infine, il disconoscimento deve essere tempestivo: deve avvenire nella prima udienza utile o nella prima risposta successiva alla rituale acquisizione della riproduzione.

caso di correzione dell'errore materiale ([29]) o di modifiche contrattuali dovute ad una successiva pattuizione tra le parti.

Il documento tradizionale è formato mediante l'utilizzo di una grandezza fisica che assume valore nel tempo, vale a dire che un documento cartaceo ha natura intrinsecamente autorevole, si tratta di un pezzo di carta che resta immutato nel tempo ([30]). Il documento è, perciò, una porzione della realtà materiale che occupa uno spazio e agisce sui sensi ([31]).

In base a quanto appena detto, si deducono i due elementi che caratterizzano questa tipologia di documento: la res corporale e il contenuto.

La prima è il supporto materiale che funge da contenitore come, ad esempio, un foglio di carta. È definito contenente, in quanto ha la funzione di trattenere la rappresentazione di un fatto, come per esempio una dichiarazione.

Nel caso del contenuto, questo è il frutto di un'attività umana sia essa spirituale o intellettuale, come ad esempio le parole che troviamo nel foglio di carta.

Per tutto ciò ne deriva che il contenuto sia inscindibile dal singolo supporto contente, a meno che non avvenga una distruzione che, inevitabilmente, comporti la separazione dei due elementi.

---

[29] L'errore materiale è l'errore dovuto a svista o disattenzione. Si tratta di un istituto del ricorso straordinario introdotto nel codice di procedura penale mediante art.625-*bis* della legge del 26 marzo 2001, n. 128. In quanto istituto del ricorso si suddivide in due articolazioni: emenda epurativa ossia l'errore materiale in senso stretto ed integrativa ossia il caso di omissione.
Affinché sia possibile ricorrere a questo strumento si identificano tre presupposti: in primo luogo si deve trattare di atti suscettibili di correzione e individuati unicamente dal giudice; l'errore non deve determinare la nullità dell'atto e la rimozione dell'errore non deve tradursi in "modificazione essenziale dell'atto".
Inoltre, sarà possibile correggere dall'errore materiale solamente gli originali dei provvedimenti giudiziali che arrecano tutti gli elementi essenziali dell'atto. Rif. GIARDA, SPANGHER; *Codice di procedura penale- commento VI edizione- tomo I*; Milano, 2023, sub art. 130 c.p.p., p. 1978 ss.

[30] Da qui sicuramente si evince il tema del supporto durevole: la carta, per esempio, è il supporto durevole per eccellenza vale a dire che è in grado di conservare ciò che le viene scritto sopra per un determinato tempo.

[31] Rif. DELFINI, FINOCCHIARO, *Diritto dell'informatica,* cit., p. 251.
Per chiarire quanto appena spiegato si rimanda anche a quanto proposto da Gianluca Navone, ricercatore di diritto privato e professore presso l'Università di Siena, nel quale spiega le fondamenta del documento tradizionalmente inteso in contrapposizione alle metafore di scrivere nell'acqua oppure di scrivere nel vento. Scrivere sull'acqua o nel vento è un chiaro paradosso. Queste parole mettono in luce il carattere immateriale dell'atto di scrivere su qualcosa che è volubile, vale a dire un attributo che non è in grado di trattenere le parole e per questo si può dire che manca di quel carattere permanente di cui gode, invece, il documento. Diversamente il documento, tradizionalmente inteso, si deve considerare come il contenitore di un'espressione linguistica, che in quanto tale si caratterizza di una materia stabile, è, cioè, in grado di fermare le parole dalla fuga del tempo. Rif. NAVONE, *Instrumentum digitale. Teoria e disciplina del documento informatico,* cit., p.54 e ss.

Tra le caratteristiche del documento vi è l'attitudine ad essere inalterabile: si tratta insomma di un bene che fornisce una rappresentazione duratura e immutabile nel tempo, anche se ovviamente può capitare che il documento sia distrutto o alterato.

Come vedremo, l'elemento del supporto durevole in rapporto alla res corporale, che caratterizza il documento analogico, assume rilevanza anche in relazione alla definizione normativa euronitaria del documento informatico.

1.3.2 GIUDIZIO SULL' AUTENTICITÀ DEL DOCUMENTO ANALOGICO

Prima di analizzare come la sottoscrizione e la certezza della data vengono assicurate in un documento analogico, si ritiene utile soffermarsi sulla questione dell'autenticità.

Il termine in questione, che dovrebbe attenere alla veridicità del documento autografo ossia alla corrispondenza fra l'autore apparente e l'autore reale, spesso viene usato con un significato diverso: autentico è il documento in grado di assumere efficacia probatoria.

1.3.2.1 SOTTOSCRIZIONE

Funzione essenziale del documento analogico, come già visto in merito alla scrittura privata, è la sottoscrizione ossia l'indicazione del nome dell'autore della scrittura.

Il processo di sottoscrizione relativo ad un documento analogico, o cartaceo, avviene grazie all'apposizione della firma autografa da parte dell'autore dello scritto; in altre parole, si tratta di quel segno grafico in grado di imputare univocamente il documento ad un determinato soggetto.

L'atto di sottoscrizione può, anche, considerarsi come una manifestazione sociale, in quanto è attraverso la firma autografa che un soggetto si assume la responsabilità, anche giuridica, di quanto scritto ([32]).

La firma autografa svolge tre funzioni:

- innanzitutto, assolve ad uno scopo dichiarativo, poiché determina l'assunzione di paternità del contenuto del documento da parte di colui che ha impresso la firma;

[32] A rafforzare quanto appena spiegato è anche la sentenza del Consiglio di Stato, sez. V, n. 3550 del 18/07/2017 dove viene ribadito che: *"La sottoscrizione di un documento è lo strumento mediante il quale l'autore fa propria la dichiarazione contenuta nello stesso, consentendo così di risalire alla paternità dell'atto e di renderlo vincolante verso i terzi destinatari della manifestazione di volontà".*

- in secondo luogo, ha natura identificativa, in quanto mira ad identificare l'autore del documento: si tratta, insomma, di uno strumento tecnico-giuridico che consente di distinguere l'effettivo autore da quelli apparenti; e
- infine, ha valore probatorio, perché dimostra la provenienza del documento dal suo autore.

Di conseguenza, si può pacificamente affermare che il documento cui sia apposta la firma autografa del soggetto che figura come autore assume valore di prova legale (rispetto alla provenienza delle dichiarazioni in esso contenute), se non vi sono state apportate successive modifiche o manomissioni e la sottoscrizione è riconosciuta, autenticata o non è stata disconosciuta. Inoltre, questo tipo di sottoscrizione, rimane inalterata nel tempo e perciò, il documento con sottoscrizione autografa conserva la propria forza probatoria nel tempo.

La firma tradizionale, perciò, prova l'assunzione di paternità della dichiarazione documentale che si compie tramite la lettura del nome del sottoscrittore in calce al documento.

La scrittura che si considera autentica vincola il giudice a ritenere che le dichiarazioni in essa contenute provengano dalle parti che le hanno firmate (ma non invece a reputarle vere).

1.3.2.1 CERTEZZA DELLA DATA

Ammesso che solo la sottoscrizione autografa è l'elemento essenziale del documento analogico, anche la data e l'ora si rivelano utili, soprattutto quando il fine è quello di provare che un determinato documento si è formato in un preciso istante temporale o che la sua esistenza era anteriore rispetto ad uno specifico evento o ad una precisa data.

Convenzionalmente la data corrisponde alla semplice scrittura del giorno, mese, anno e alla scrittura del nome del comune in cui la dichiarazione è stata resa.

Spesso però capita che non venga apposta la data oppure che non vengano riportati gli elementi previsti dall'art 2704 c.c. rubricato "*data della scrittura privata nei confronti dei terzi"* in merito alla considerazione della data certa e la sua opponibilità nei confronti dei terzi.

Per questo motivo si può pacificamente affermare che la catalogazione contenuta nella norma appena citata non sia tassativa e che l'opponibilità della data nei confronti dei terzi possa essere garantita anche mediante altri elementi.

Ad esempio, è ritenuta idonea a conferire data certa la morte o la sopravvenuta impossibilità fisica di colui o di uno di coloro che hanno sottoscritto il documento ovvero la riproduzione della scrittura in atti pubblici. (v. *supra* le prove documentali, la scrittura privata).

1.4 IL DOCUMENTO INFORMATICO

Con l'avvento delle nuove tecnologie digitali il concetto di documento tradizionalmente inteso, in quanto direttamente correlato ad un supporto materiale tangibile, è stato riformulato e dalla sua rilettura in chiave moderna è nato il documento informatico.

1.4.1 DEFINIZIONI E PECULIARITÀ DEL DOCUMENTO INFORMATICO

La definizione di documento informatico fa un timido ingresso nel campo legislativo nazionale con la legge n.59 del 1997, la c.d. "legge Bassanini 1", all'articolo 15 co.2, dove si introduce per la prima volta il concetto di documento informatico e la sua validità a tutti gli effetti di legge ([33]).

La definizione del documento informatico o elettronico si rinviene sia nella normativa nazionale che in quella comunitaria.

In Italia, il Codice dell'Amministrazione Digitale (di seguito denominato più semplicemente CAD) disciplina il concetto di documento informatico mettendone in luce la sua rilevanza dal punto di vista giuridico all'articolo 1 lett. p. ([34]).

A livello europeo, con la pubblicazione del Regolamento UE n.910 del 2014, meglio noto come Reg. eIDAS (*Electronic Identification Authentication and Trust Services*), il cui fine è quello di uniformare la disciplina generale in materia di strumenti informatici e

---

[33] *"1. […] 2. Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonche' la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalita' di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati […]"*
La necessità di introdurre il termine documento informatico è legata ad un aspetto culturale poichè tradizionalmente al termine documento si affianca il termine cartaceo. Inoltre, la scelta del legislatore italiano risulta inutile rispetto agli insegnamenti di Carnelutti nei quali sostenva che: "*qualunque materia, atta a formare una cosa rappresentativa, può entrare nel documento: tela, cera, metallo, pietra e via dicendo*". Rif. DELFINI e FINOCCHIARO, *Diritto dell'informatica*, cit., p. 311.

[34] *"p) documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti."*

telematici, descrive il documento elettronico, all'art.3 n.35, ne evidenziandone la sua funzione principale ossia quella di contenitore di atti o fatti ([35]).

Che l'evoluzione tecnologica permetta alle persone di manifestare le proprie dichiarazioni in forma digitale è ormai una constatazione banale.

La rappresentazione della realtà che prima dell'avvento di internet avveniva principalmente con il documento analogico e derivava quindi dall'utilizzo di idiomi; è ora astratta e numerica. Tutto ciò che viene creato dall'uomo per mezzo di un computer è un artefatto informatico, che assume rilevanza mediante strumenti e astrazioni computazionali ([36]).

Le astrazioni ci permettono di rappresentare una vasta varietà di dati, generalmente rappresentati mediante zeri e uno, si tratta dei c.d. *bit* ([37]). Questi creano pattern di dati, che a loro volta vengono associati a dei valori numerici, i quali assumono rilevanza in base al contesto in cui si trovano.

A titolo illustrativo, sembra interessante spiegare, seppur brevemente, quali siano i fondamenti di una rappresentazione testuale.

Innanzitutto, le informazioni vengono codificate in zero e uno, perciò, le lettere dell'alfabeto e i segni di interpunzione saranno associati ad un pattern univoco di bit ([38]).

Per evitare l'insorgenza di problemi dovuti alla mancanza di codici univoci per decifrare i segni, l'Istituto Nazionale Americano per la standardizzazione ha adottato il codice ASCII, *American Standard Code for Information Interchange.* Quest'ultimo permette la rappresentazione numerica dei caratteri alfanumerici ed è grazie a questo codice che

---

[35] *"«documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva."*

[36] Il tema della permanenza della rappresentazione documentale costituisce un effetto riflesso della durevolezza esteso anche per i documenti informatici. Già con la Direttiva 97/7/CE al Considerando 13 viene citato il concetto di "supporto durevole": "*considerando che l'informazione diffusa da talune tecnologie elettroniche ha spesso un carattere effimero in quanto essa non è ricevuta su un supporto durevole; che è necessario che il consumatore riceva, in tempo utile, per iscritto, informazioni necessarie ai fini della buona esecuzione del contratto*". L'interpretazione estensiva appare là dove per supporto durevole si intenda anche qualsiasi altro strumento, comprese soluzioni tecniche, in grado di equivalere ad un'informativa redatta su un foglio di carta. (Corte di Giustizia dell'UE, sez. III, causa n. 49 del 05/07/2012).

[37] I bit, *binary digit,* sono le informazioni codificate mediante zero e uno. Si tratta di semplici simboli il cui valore assume rilievo in base alle base al contesto nel quale vengono utilizzati, vale a dire che possiamo parlare di bit che rappresentano un testo dove ogni lettera dell'alfabeto è ricollegata ad un determinato simboli, altre volte possono rappresentare immagini, colori o ancora suoni. Rif. BROOKSHEAR e BRYLOW, *Informatica, Una panoramica generale*, Milano, 2020, p. 22.

[38] Rif. BROOKSHEAR e BRYLOW, *Informatica, Una panoramica generale*, cit., p. 35 e ss.

siamo in grado, oggi, di poter scrivere una lunga sequenza di simboli codificati detti anche file di testo.

I dati informatici non sono paragonabili ai dati sottoscritti in un documento, in quanto per la loro stessa natura sono facilmente modificabili e volatili, basta, infatti, una semplice azione per trasformarli senza avere più la possibilità di recuperali.

Inoltre, sono deteriorabili e distruttibili, cioè se non maneggiati con le adeguate accortezze questi possono essere danneggiati o addirittura persi per sempre.

Per tutti questi motivi si vede la necessità di garantire determinati requisiti tecnici di qualità e sicurezza per la creazione del documento informatico e di integrità e immodificabilità per il documento stesso.

A ben vedere già all'epoca il Decreto del Presidente della Repubblica (d.p.r.) n.445 del 2000 all'art. 52, prevedeva i requisiti da rispettare per la gestione informatica dei documenti ([39]).

Interessante sarà quindi richiamare l'attenzione sul fatto che il compimento di questo atto giuridico in forma digitale ha come conseguenza la formazione di un documento informatico in grado di produrre effetti giuridici, come in seguito analizzeremo.

1.4.1.1 DOCUMENTO ELETTRONICO, INFORMATICO E DIGITALE: DIFFERENZE

Nell'economica del presente lavoro si ritiene utile analizzare, brevemente, la differenza tra le diverse accezioni sottese alle locuzioni «documento elettronico», «documento informatico» e «documento digitale», che vengono spesso utilizzate come interscambiabili, anche se in realtà non coincidono perfettamente.

---

[39] *"1. Il sistema di gestione informatica dei documenti, in forma abbreviata "sistema" deve:*
a) garantire la sicurezza e l'integrità del sistema;
b) garantire la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita;
c) fornire informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati nell'adozione dei provvedimenti finali;
d) consentire il reperimento delle informazioni riguardanti i documenti registrati;
e) consentire, in condizioni di sicurezza, l'accesso alle informazioni del sistema da parte dei soggetti interessati, nel rispetto delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
f) garantire la corretta organizzazione dei documenti nell'ambito del sistema di classificazione d'archivio adottato".

Il Reg. eIDAS affianca al termine documento l'aggettivo elettronico, ponendo così l'attenzione sia sul contenuto che sul contenitore.

L'art. 3 n.35 del reg. cit. prevede che "*qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva"*. È evidente che il requisito fondamentale affinché ci si possa riferire a un documento elettronico è che il contenuto, qualunque esso sia, sia in formato elettronico.

Il formato elettronico riguarda la scienza dell'elettronica ossia quell'insieme di conoscenza metodologiche, tecniche e pratiche che, mediante la progettazione e la realizzazione di sistemi hardware e software, sono in grado di elaborare grandezze fisiche sottoforma di segnali contenenti informazioni.

Invece, il contenitore sarà necessariamente legato al progresso tecnologico: se prima un documento elettronico aveva più possibilità di essere salvato su un DVD o un CD, ora è più probabile che questo si trovi all'interno di una chiavetta usb, anche nota come *pen drive*.

La scelta del legislatore europeo è chiara: definisce solo l'aspetto tecnologico del documento elettronico, in questo modo la definizione appare generica e ogni Stato membro avrà la possibilità di interpretare il documento elettronico e i suoi effetti giuridici (chiaramente sempre nel rispetto del principio della irrilevanza della materia) in base al proprio contesto giuridico.

Quanto alla definizione a livello italiano il termine disciplinato nella normativa di riferimento è quello di documento informatico. L'art. 1 lett. p ([40]) si concentra sull'attitudine del documento informatico a rappresentare fatti che siano giuridicamente rilevanti. Pertanto, il documento informatico in sé non è assoggettato al supporto fisico che lo contiene, vale a dire che l'accesso alle informazioni in esso contenute può avvenire mediante un computer o altro mezzo idoneo. Attenzione però che, se anche il supporto fisico non è accuratamente normato dal legislatore, risulta comunque necessario, infatti, diversamente non si potrebbe leggere il contenuto del documento.

L'informatica, tra l'altro, è la scienza che riguarda lo studio delle informazioni nella loro totalità, sia dalle informazioni come input quindi le caratteristiche di immissione delle

[40] *"p) documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.".*

stesse in un algoritmo con riguardo alla loro struttura; l'algoritmo che le trasforma e l'output prodotto.

Da ultimo, il documento digitale richiama la sua attitudine a rappresentare informazioni tramite un apposito sistema di numerazione informatico. Il termine digitale, come ci suggerisce il Vocabolario della lingua italiana Treccani ([41]), è associato ad apparecchi e dispositivi che lavorano con un sistema di numerazione, quello più comune è detto binario.

Riassumendo, il concetto presupposto nella normativa europea di documento elettronico pone l'attenzione sugli apparati, che tuttavia non sono regolamentati, se non nella misura in cui devono obbligatoriamente essere in grado di elaborare informazioni in formato elettronico.

Con la definizione data dal legislatore italiano di documento informatico invece ci si concentra sull'aspetto delle informazioni: l'importante, secondo questo approccio, è che queste siano giuridicamente rilevanti.

Infine, nella nozione di documento digitale pone la lente d'ingrandimento sul sistema delle informazioni rappresentate mediante cifre di un determinato sistema di numerazione.

Nella presente disamina il termine utilizzato sarà quello di documento elettronico così da adeguarsi al Reg. eIDAS.

1.4.2 VALIDITÀ GIURIDICA

Come già accennato, con la legge Bassanini 1 l'ordinamento italiano aveva già riconosciuto il documento informatico, disciplinandone alcuni aspetti relativi alla formazione, all'archiviazione, all'esibizione e alla trasmissione telematica.

La valenza giuridica del documento elettronico viene ribadita naturalmente anche nel Regolamento eIDAS, al Considerando 63, ove si legge che *"I documenti elettronici sono importanti per l'evoluzione futura delle transazioni elettroniche transfrontaliere nel mercato interno. Il presente regolamento dovrebbe stabilire il principio secondo cui a un documento elettronico non dovrebbero essere negati gli effetti giuridici per il motivo nella*

[41] https://www.treccani.it/vocabolario/digitale2/

sua forma elettronica al fine di assicurare che una transazione elettronica non possa essere respinta per il solo motivo che un documento è in forma elettronica".

Ciò detto, è opportuno sottolineare che il valore giuridico del documento informatico, che, come abbiamo appena visto, è indipendente dal supporto fisico nel quale è contenuto, è diversamente, considerato soprattutto in ragione della tipologia di firma che eventualmente vi è apposta, come meglio vedremo nel seguente paragrafo.

Se il legislatore europeo ha deciso di uniformare la materia dell'identità digitale e dei servizi ad essa connessi in maniera tecnologicamente neutrale e in modo tale da lasciare un certo raggio d'azione a ciascun Stato membro, è essenziale conoscere la normativa nazionale per mettere bene a fuoco la validità giuridica di un documento informatico ([42]).

In Italia la norma di riferimento è rappresentata dall'art.20 del Codice dell'Amministrazione Digitale, così come modificato dal decreto legislativo in 13 dicembre 2017, n. 217 ([43]), ai sensi del quale *"Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida".*

In base al dettato normativo è chiaro che un documento informatico privo di sottoscrizione sia liberamente valutabile dal giudice che mediante un'attenta valutazione discrezionale ed effettuata a posteriori deciderà se il documento *de qua* possa integrare la

[42] Qualora si volesse approfondire l'oggetto e l'ambito di applicazione del Regolamento cit. si consiglia: DALMARTELLO E SALVEMINI, *Oggetto e ambito di applicazione,* in DELFINI e FINOCCHIARO (a cura di), *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, Torino, 2017.

[43] Per un confronto in merito al testo originario dell'art. 20 e 21 del Codice dell'Amministrazione Digitale con gli articoli in vigore si veda la tabella comparativa: GIACALONE, *Il ciclo di vita di un documento informatico: gestione e aspetti normativi*, Milano, 2021, p.73

forma scritta in generale e quale sia il suo valore probatorio anche in relazione alle caratteristiche oggettive del documento ([44]).

Invece, all'art. 21, co.1-*bis*, CAD si specifica che la forma scritta *ad substantiam,* è soddisfatta quando il documento informatico è sottoscritto mediante firma elettronica avanzata, qualificata o digitale ovvero sono formati con ulteriori modalità di cui all'art. 20, co.1-*bis*, primo periodo ([45]) (v. *sotto* par. effetti giuridici).

1.4.3 SOTTOSCRIZIONE

Si è visto che già la Direttiva n.93 del 1999 cercava di fornire un quadro normativo di riferimento, a livello comunitario, per le firme elettroniche. Tale Direttiva è stata poi abrogata dal Reg. eIDAS attualmente vigente, che ha apportato delle innovazioni significative in merito alla definizione di firma elettronica. Quest'ultima è descritta dall'art. 3 del cit. Reg. quale insieme di dati elettronici utilizzati "per firmare", diversamente da quanto prevedeva la direttiva del 1999, che discorreva di "*dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione"*. Questa riformulazione terminologica testimonia il tentativo del legislatore europeo di avvicinare la definizione della firma elettronica a quella della tradizionale sottoscrizione autografa; dal menzionato disposto del Reg. emerge infatti, chiaramente, la volontà di considerare la prima non come un mezzo di identificazione (in linea con quanto già stabiliva la precedente direttiva), bensì piuttosto, come un vero e proprio "strumento per firmare".

A livello nazionale, nella nuova versione del CAD, a seguito delle modifiche apportate dal d.lgs. 26 agosto 2016, n. 179, la definizione di firma elettronica è stata soppressa, in

---

[44] Tra le tante, si riporta qui la massima della sentenza più recente in materia di documento informatico privo di sottoscrizione. In particolare, nel caso in esame, si trattava di una e-mail semplice e in quanta tale priva di quei requisiti idonei a ricollegare in modo univoco e con un elevato livello di certezza la firma al firmatario, nel caso di specie il login con nome utente e password sarebbe assimilabile ad una firma elettronica semplice.
La massima: "*Il messaggio di posta elettronica (cd. e-mail) privo di firma elettronica non ha l'efficacia della scrittura privata prevista dall'art. 2702 c.c. quanto alla riferibilità al suo autore apparente […]. E la sottoscrizione costituita dalla firma del dichiarante, […], in caso di documento informatico, dalla firma elettronica avanzata, qualificata o digitale, rappresenta l'espressione grafica della paternità ed impegnatività della dichiarazione che la precede, la quale in mancanza non comporta la conclusione definitiva di un negozio giuridico allorché la forma scritta sia richiesta ad substantiam. Pertanto, una e-mail che contenga espressioni generiche di consenso ma sia priva della firma elettronica avanzata, qualificata o digitale dei promittenti, non integra l'atto scritto richiesto dagli artt. 1350 e 1351 c.c.".* Rif. Cass. Civ., sez.II, sentenza n. 22012 del 24/07/2023, in *DeJure.it.* .
[45] Rif. CASADEI e PIETROPAOLI, *Diritto e tecnologie informatiche*, Trento, 2021, p. 81.

quanto come ben si sa, le disposizioni dei regolamenti UE sono direttamente applicabili all'interno dei sistemi dei singoli Stati membri.

L'uso della firma elettronica dovrebbe essere strettamente personale, in quanto serve a identificare la persona fisica che sottoscrive un determinato documento.

Poiché l'attribuzione della firma elettronica è limitata alle sole persone fisiche, qualora un documento debba essere sottoscritto da una persona giuridica, questa potrà avvalersi del sigillo elettronico ([46]).

Ad ogni modo, appare utile comprendere quale sia la validità e l'efficacia giuridica della firma elettronica, in modo da valutare se quest'ultima rappresenti una mera evoluzione della sottoscrizione autografa oppure dia luogo a qualcosa di diverso.

1.4.3.1 TIPOLOGIE DELLE FIRME ELETTRONICHE

Le firme elettroniche costituiscono una categoria aperta nel Reg. eIDAS, in quanto vincolate al progresso tecnologico.

Il progredire delle tecnologie informatiche è sempre più rapido e normare in maniera dettagliata una tecnologia utilizzata, in un determinato momento, presupporrebbe un atto di normazione ristretto, in quanto sarà inesorabilmente destinata ad essere potenziata.

Perciò il legislatore comunitario ha deciso di normare in maniera generica la disciplina, in modo tale da, ricomprendere non solo le tecnologie attuali al momento della legiferazione ma anche quelle "futuribili" ([47]).

---

[46] *Art. 3 n.25 Reg. eIDAS: "«sigillo elettronico», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi".* Il sigillo elettronico è lo strumento che serve per autenticare i documenti informatici appartenenti ad una persona giuridica (v. C-65 del Reg. cit.). Nonostante sia spesso considerato come la firma elettronica della persona giuridica, è utile ricordare che però questa affermazione non è del tutto corretta. Infatti, se come visto in seguito alla firma elettronica svolgere tre funzioni per il sigillo elettronico non è lo stesso. Le funzioni di quest'ultimo sono dunque due: la funzione identificativa, vale a dire che identifica la persona giuridica alla quale appartiene il sigillo apposto, e quella probatoria, chiaramente ai fini probatori ciò significa che produce prova della provenienza del sigillo. Per approfondire il tema: DELFINI e FINOCCHIARO (a cura di), *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno,* cit., p. 257 ss.

[47] Le firme elettroniche sono classificabili secondo diversi criteri ovvero in base alle modalità di formazione, alle finalità perseguite o alle proprietà loro attribuite. In relazione alle classificazioni di firme elettroniche si ricorda quella effettuata da UNCITRAL in particolare nel *Model Law on Electronic Signatures with Guide to Enactment* (di seguito MLES), suddivide le firme in base al meccanismo di autenticazione operato dall'utente. Si potrà avere autenticazione sulle basi di conoscenza dell'utente (*something you konw),* sulle carattertistiche fisiche (*something you are)* e rispetto al possesso di un oggetto da parte dell'utente (*something you have).*

In base a quanto previsto dalla normativa comunitaria sono tre le tipologie di firma elettronica individuate:

- la firma elettronica semplice,
- la firma elettronica avanzata,
- la firma elettronica qualificata.

La firma elettronica semplice, detta anche "debole" è la tipologia di sottoscrizione elettronica più elementare prevista dalla normativa comunitaria e corrisponde a "*dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare*".

La firma elettronica semplice più nota è quella che deriva dal meccanismo *Point& Click* e corrisponde al *click* ossia alla pressione su un pulsante che l'utente fa dopo essersi autenticato mediante userID e password. Si tratta di un sistema che non è in grado di garantire la riconducibilità univoca della firma al firmatario, infatti, sarà banale ricordare che le credenziali possono essere facilmente dimenticate dall'utente o anche perse. Perciò il fatto che l'utente non abbia il controllo esclusivo circa l'userID e password o meglio il controllo può essere facilmente limitato è uno dei motivi principali per i quali la firma in esame è considerata debole.

Questo tipo di firma si basa su una tecnologia neutra ([48]), come in seguito vedremo lo stesso vale per la firma elettronica avanzata.

La firma elettronica avanzata offre un maggior livello di sicurezza solo quando risultino soddisfatti i requisiti previsti dall'art. 26 del Reg. eIDAS ossia:

- la connessione univoca al firmatario,
- è idonea ad identificare il firmatario,
- la creazione della firma elettronica deve essere sotto l'esclusivo controllo del firmatario
- e infine, ogni ulteriore modifica dei dati deve essere conosciuta. ([49])

[48] Si tratta di un particolare approccio normativo, noto anche con il termine inglese di *functional equivalent* o *technology neutral*, in base al quale le definizioni di firma sono pensatamente vaghe e molto generiche in modo tale da poter ricomprendere nel dettato ogni possibile, presente e futura, evoluzione tecnologica, evitando così anche il fenomeno dell'obsolescenza tecnologica. Rif. *Model Law on Electronic Signatures with Guide to Enactment 2001,* United Nations, New York, 2002.

[49] *"Una firma elettronica avanzata soddisfa i seguenti requisiti:*

a) è connessa unicamente al firmatario;

La firma grafometrica è un perfetto esempio di firma elettronica avanzata, viene spesso utilizzata nel settore assicurativo o bancario. L'utente per apporre la sua firma elettronica dovrà fare un gesto manuale, lo stesso che emula nel caso in cui dovesse firmare con una penna su carta, con l'unica differenza che la superficie sulla quale dovrà emulare il gesto sarà un tablet. Quando eseguito il gesto, lo schermo mediante dei sensori sarà in grado di rilevare una serie di dati utili ([50]).

Per il procedimento appena spiegato si può pacificamente affermare che la firma grafometrica e perciò anche la firma elettronica avanzata è in grado di garantire la connessione univoca della firma al firmatario.

La firma elettronica qualificata, detta "forte" e disciplinata all'art. 3 n.12 del Reg. cit. ([51]); si basa su un certificato qualificato in grado di garantire con certezza l'identità del soggetto che firma il documento, assicurando anche l'integrità e l'immodificabilità del documento dopo la sottoscrizione.

La tecnologia utilizzata per questo tipo di firma non è più basata su un tipo di tecnologia neutra, che coma già visto era in grado di adattarsi all'evoluzione tecnologica, bensì si basa su un sistema PKI (Public Key Infrastracture) o infrastruttura a chiave pubblica ([52]) di cui il certificato è l'elemento essenziale ([53]). Questa tecnica di cifratura prevede

---

b) è idonea a identificare il firmatario;
c) è 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) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati".

[50] Tra i dati utili che si possono rilevare dall'apposizione di una firma elettronica su un tablet si trovano: i canali di posizione della punta della penna sul piano di firma (coordinate X, Y, Z rispetto alle coordinate dello spazio), il canale del tempo trascorso dalla primo campione di firma considerato (coordinata T) oppure la differenza di tempo trascorsa tra due campionamenti consecutivi (coordinata DT), o ancora la pressione ossia la forza applicata sulla penna dal piano di firma (coordinata F). Questi appena elencati sono tutti dati biometrici utili ad identificare il firmatario e che si ricavano dall'apposizione di una firma grafometrica. Rif. ISO 19794/7.

[51] "*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".*

[52] In riferimento a quanto previsto ITU-T X.509 (l'International Telecommunication Union ossia l'agenzia degli Stati Uniti specializzata nel campo delle ICT) la PKI è l'infrastruttura creata per supportare l'emissione, la revoca e la convalida dei certificati a chiave pubblica; la validazione, tra le diverse cose, verifica il certificato di firma digitale. Il processo prevede che il firmatario crei la sua firma elettronica e la cripti con la chiave privata mentre il validatore la verificherà con la chiave pubblica. Se al momento della verifica risulta che i dati all'interno del messaggio cifrati sono stati modificati allora il processo sarà dichiarato invalido, altrimenti sarà considerato valido.

[53] Per approfondire il tema del certificato di firma elettronica qualificata: LODI, *Certificati qualificati di firme elettroniche* e *Requisiti relativi ai dispositivi per la creazione di una firma elettronica qualificata,* in DELFINI e FINOCCHIARO (a cura di), *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, cit.

l'utilizzo di due differenti tipologie di chiavi, quella pubblica necessaria per cifrare un messaggio e quella privata utilizzata, invece, solamente per decifrare (viceversa la chiave per cifrare può essere quella privata e quella per decifrare sarà la chiave pubblica), in questo modo si garantisce la massima sicurezza ai messaggi cifrati.

1.4.3.2 FUNZIONI DELLE FIRME ELETTRONICHE

Se come già analizzato sono tre le funzioni che si possono associare alla sottoscrizione autografa, per quella elettronica la situazione è più complessa.

Da subito è essenziale chiarire che sebbene la firma elettronica e la sottoscrizione autografa sembrino riferirsi a concetti equipollenti, nella realtà rimangono delle differenze notevoli tra essi. La diversità non è solo di tipo tecnico (la firma autografa è un gesto umano vincolato a "carta e inchiostro" mentre quella elettronic è di derivazione tecnologica), ma anche di tipo giuridico.

Se alla sottoscrizione autografa è ricollegata la funzione identificativa, dichiarativa e probatoria non si può dire lo stesso per la firma elettronica. Sicuramente a quest'ultima sarà riconosciuta la funzione identificativa e dichiarativa mentre quella probatoria trova qualche difficoltà soprattutto in relazione alla mancanza di consapevolezza che l'apposizione di una firma elettronica porta con sé.

Allo stesso modo, alcune tipologie di firma elettronica garantiscono funzioni che le tradizionali firme autografe non possono assicurare o sono assicurate in maniera differente. Ad esempio, in riferimento ad una firma elettronica qualificata l'identificazione del firmatario viene assicurata in maniera diversa rispetto ad una sottoscrizione autografa, poiché la certificazione è assicurata da un soggetto qualificato.

Sicuramente la firma elettronica è in grado di assicurare la funzione di identificazione del soggetto, firmatario, distinguendolo dagli altri proprio come per la firma tradizionale dove si individua l'autore del documento. Il firmatario è "*una persona fisica che crea una firma elettronica*" e la firma elettronica è un'associazione logica di dati in formato elettronico necessaria al soggetto stesso per, appunto, firmare un documento ([54]).

[54] L'identificazione elettronica del soggetto ricopre un ruolo fondamentale all'interno del Regolamento eIDAS tanto che si preoccupa di chiarire subito la differenza con l'autenticazione elettronica. La prima riguarda il processo di dati che rappresentano una persona fisica o giuridica mentre la seconda è solo un processo di derivazione, serve infatti solo per confermare l'identificazione elettronica. Rif. DELFINI e FINOCCHIARO, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno,* cit., p. 16.

Inoltre, questa funzione appare rafforzata quando si pensa ad una firma elettronica qualificata poiché, dal punto di vista tecnico, verrà rilasciato un certificato qualificato dal prestatore di servizi garantendo l'identificazione del soggetto.

L'altra funzione espressamente richiamata dal Regolamento è quella probatoria. Con riferimento alla normativa italiana, la funzione in esame appare rafforzata per le firme elettroniche qualificate e per le firme digitali dal momento che è previsto inversione dell'onere della prova. Se come già visto tradizionalmente chi deve provare un fatto è anche colui che deve dimostrare le prove dell'esistenza del fatto stesso; ora la situazione appare differente. Come previsto dall'art. 20, comma 1-ter CAD: "*L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria"* ([55]).

La funzione dichiarativa, ossia quella che riguarda l'espressione del consenso rispetto al contenuto del documento, non è immediatamente richiamata dal Regolamento e sembra essere attenuata in confronto alla sottoscrizione autografa. Quando un soggetto fa il gesto fisico di firmare sembra più consapevole di quello che sta facendo di quanto non lo sia la cosa che invece appare affievolita nel momento dell'apposizione della firma elettronica ([56]).

1.4.3.3 EFFETTI GIURIDICI DELLE FIRME ELETTRONICHE

Per quanto concerne gli effetti giuridici della firma è necessario chiarire che sono disciplinati sia a livello del diritto dell'UE, dal Reg. eIDAS che a livello nazionale; chiaramente in base alla diversa tipologia di firma apposta si avranno differenti effetti giuridici.

A livello comunitario, all'art. 25 del Reg. eIDAS, si delineano i presupposti circa la validità giuridica della sottoscrizione elettronica ([57]).

---

[55] Quanto alle funzioni della firma elettronica queste sono ribadite anche MLES all'art.6 rubricato "*compliance with a requirement for a signature".* (par.73).

[56] Quello che si rileva è una mancanza di consapevolezza sia in merito all'apposizione della firma elettronica stessa che in relazione agli effetti giuridici che questa può comportare. Rif. DELFINI e FINOCCHIARO, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno,* cit., p. 219.

[57] *"1. A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.*
2. Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.
3. Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri".

Al comma primo si ribadisce ancora una volta il principio del riconoscimento della firma elettronica ([58]). Al comma secondo è disciplinata la firma elettronica qualificata: questa è equiparata alla sottoscrizione autografa (v. *supra* sottoscrizione). All'ultimo comma viene in risalto il principio dell'interoperabilità giuridica ([59]).
Si deve al legislatore nazionale la delineazione più precisa degli effetti giuridici derivanti dall'apposizione di una firma elettronica. Il cuore della disciplina è l'art. 20, co.1-*bis* del Codice dell'Amministrazione Digitale ([60]). La norma in esame disciplina i diversi effetti giuridici in base alla tipologia di sottoscrizione elettronica.

In base a quanto previsto dalla prima parte del comma, un documento informatico sottoscritto con firma elettronica avanzata, qualificata o firma digitale ha la medesima efficacia probatoria riconosciuta alla scrittura privata ai sensi dell'art. 2702 c.c.

Non solo, perché il paragrafo spiega poi che anche un documento formatosi mediante identificazione dell'autore, creatosi rispettando i requisiti fissati dall'AgID ([61]) e rispettando i requisiti oggettivi del documento può avere gli stessi effetti giuridici riconosciuti ad una scrittura privata.

Qualora, invece, il documento fosse privo di sottoscrizione ovvero sia firmato mediante firma elettronica semplice allora sarà oggetto del prudente apprezzamento del giudice che fonderà le proprie considerazioni anche in base ai requisiti oggettivi del documento.

---

[58] Il riconoscimento del principio del non disconoscimento della firma elettronica venne già anticipato nella Convenzione delle Nazione Unite sull'uso delle comunicazioni elettroniche nei contratti internazionali nel 2005 all'art. 8 rubricato "*legal recognition of electronic communications".* Vedi anche DELFINI e FINOCCHIARO, *Diritto dell'informatica*, cit., p.46.

[59] Il concetto di interoperabilità è una nozione complessa e composta da diverse sfaccettature di significato. Brevemente si dice che il legislatore europeo pone alla base delle comunicazioni elettroniche il principio dell'interoperabilità tra Stati membri e in un'ottica di sviluppo per il *Digital Single Market*. Per approfondire il tema: SODDU, *Cooperazione e interoperabilità,* in DELFINI e FINOCCHIARO (a cura di), *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno,* cit.

[60] *"1-bis. Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida."*

[61] L'AgID è l'organismo di vigilanza pubblico italiano e il suo compito nel caso in esame sarà quello di adottare le *Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del presente Codice.* Le Linee guida si possono consultare facilmente sul sito internet dell'Agenzia per l'Italia digitale.

Per completezza occorre nominare anche un'ulteriore tipologia di sottoscrizione elettronica: la firma digitale. Si tratta di una declinazione puramente nazionale, infatti non è prevista a livello comunitario e rientra nella categoria delle firme elettroniche qualificate per le sue caratteristiche intrinseche. È una firma dalla tecnologia non neutra che si basa su tecniche crittografiche in grado di garantire il maggior livello di sicurezza tra le firme elettroniche. (v. *supra* tipologie)

È disciplinata all'art. 1 lett. s. del CAD ([62]) e anche questa, essendo una tipologia di firma elettronica qualificata si basa su certificato qualificato rilasciato da un prestatore di servizi fiduciari.

Il ragionamento fatto fino ad ora in merito agli effetti giuridici che l'apposizione ad un documento una firma elettronica comporta riguardano i documenti informatici dichiarativi. Esistono però anche i documenti informatici non dichiarativi. Questi sono quelli, ad es., che rappresentano immagini o suoni riprodotti, e costituiscono delle riproduzioni informatiche disciplinate dall'art. 2712 c.c. Qualora non vi sia disconoscimento dalla parte contro cui è prodotto il documento informatico, si presuppone la corrispondenza al vero delle immagini ovvero la conformità di una dichiarazione resa in formato digitale ma priva di sottoscrizione.

1.4.3.4 CREAZIONE, CERTIFICAZIONE E CONVALIDA DELLE FIRME

Per quanto detto fino a questo momento è utile ricordare che l'apposizione della firma elettronica implica una serie di attività, la prima delle quali è costituita dalla creazione.

La fase di creazione non è universale poiché, come si è visto fino ad ora, esistono diverse tipologie di firme. Nei casi più elementari la firma elettronica presuppone solo la creazione di una *password* da parte del firmatario e quindi consiste nella mera composizione di una sequenza di caratteri alfanumerici e simboli. Per altre tipologie di firme servirà predisporre un dispositivo appropriato per la creazione definito dal Regolamento cit. come "*un software o hardware configurato utilizzato per creare una*

[62] "*s) 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 di firma elettronica tramite la chiave privata e a un soggetto terzo 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".*

firma elettronica" ([63]) o, ancora, potrebbe essere necessario l'intervento di un soggetto abilitato *ad hoc* ciò ossia del c.d. "prestatore di servizi fiduciari".

La firma elettronica creata deriva dall'associazione di dati che rendono riconducibile il firmatario ad una determinata sottoscrizione digitale, ma la sicurezza con cui si può constatare questa riconducibilità varia a seconda della tipologia di firma utilizzata.

A seguito della fase di creazione, alcune firme devono sottoporsi ad una ulteriore attività di certificazione in modo tale da garantire il collegamento biunivoco tra la persona fisica identificata e la firma elettronica. A questo fine si rimanda all'art 3. n. 14 del Regolamento cit. ([64]).

Il risultato di questa ulteriore attività di certificazione è il "certificato di firma elettronica", semplice o qualificato. Il certificato di firma è un attestato elettronico che collega i dati di convalida della firma elettronica ad una certa persona fisica. Qualora, invece, il certificato fosse inerente ad una firma elettronica qualificata allora si parlerà di "certificato qualificato di firma elettronica" ([65]).

Ulteriore attività necessaria questo processo di creazione della firma elettronica è l'attività di convalida, normata all'art. 3 n.41 della norma in esame ([66]).
Si tratta di un'operazione fondamentale qualora si voglia assicurare che il documento informatico sia stato validamente sottoscritto. È infatti la validità del certificato di firma elettronica che consente al documento a cui è apposta di avere determinati effetti giuridici ([67]).

---

[63] L'allegato II del Regolamento rubricato *Requisiti per i dispositivi per la creazione di una firma elettronica qualificata* prevede che, tra le diverse cose, sia assicurata la riservatezza dei dati per la creazione della firma e che i dati devono comparire una sola volta. Perciò per garantire un elevato livello di sicurezza i dati utilizzati non possono essere derivati e devono essere protetti contro l'uso da parte di terzi.

[64] *"«certificato di firma elettronica», un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona".*

[65] In base a quanto previsto dall'Allegato II del Regolamento cit. in materia di requisiti per i certificati qualificati è previsto che ci siano alcune indicazioni necessarie. Tra le quali, deve essere indicato almeno il nome del firmatario o un suo pseudonimo, i dati di convalida che corrispondono ai dati per la creazione della firma elettronica e ancora, il periodo di validità del certificato con data di inizio e fine.

[66] *"«convalida», il processo di verifica e conferma della validità di una firma o di un sigillo elettronico".*

[67] Gli effetti giuridici previsti a livello nazionale non sono gli unici che possono essere assicurati alla convalida. Infatti, questa è importante anche nell'ottica dell'interoperabilità prevista dal Regolamento. Più in particolare ci si riferisce alla possibilità che una firma elettronica creata e convalidata in uno Stato membro dell'Unione possa essere riconosciuta anche in un altro Stato membro. Per approfondire il tema: CANDINI, *Riconoscimento reciproco,* in DELFINI e FINOCCHIARO, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno,* cit.

Chiaramente, qualora il certificato di firma dovesse scadere, anche il documento a cui la sottoscrizione è stata apposta perderà di efficacia probatoria, come previsto ai co. 4 e 5 dell'art. 28 del Reg. cit. ([68]).

Perciò se, come spiegato nel precedente paragrafo, il documento informatico a cui è stata apposta una firma digitale valida gode della stessa efficacia probatoria della scrittura privata ai sensi dell'art. 2702 c.c.; qualora il certificato di firma scada allora l'efficacia probatoria di cui gode il documento in esame non sarà più la stessa. Infatti, in questo ultimo caso il documento è assimilabile alla stessa efficacia probatoria che gode una riproduzione informatica ai sensi dell'art. 2712 c.c.

Per questo motivo sarà necessario analizzare quali siano le tecniche utilizzate per evitare la diminuzione dell'attitudine probatoria del documento informatico.

1.4.4 RIFERIMENTO TEMPORALE: breve introduzione

Se il documento analogico è in grado di mantenere la sua efficacia probatoria illimitata nel tempo grazie alla sottoscrizione autografa, lo stesso non si può dire per la sottoscrizione elettronica, che come appena esaminato si differenzia per avere un certificato di firma suscettibile di scadenza dopo tre anni.

Alla stregua delle considerazioni svolte, sembra che l'apposizione della marca temporale sia una delle possibilità ad oggi disponibili per evitare che il documento informatico perda della sua efficacia probatoria.

Un modo per garantire data certa ad un documento informatico è la validazione temporale elettronica, tema che verrà ampiamente analizzato nel prossimo capitolo. La validazione temporale elettronica, come previsto sia dalla normativa comunitaria che da quella nazionale, è uno strumento atto a indicare il momento preciso in cui un documento informatico è stato creato, trasmesso o archiviato e ne garantisce la sua validità nel tempo chiaramente quando rispettai i requisiti previsti dalla Regolamento eIDAS.

---

[68] *"[…] 4. Qualora un certificato qualificato di firme elettroniche sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.*
5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea di un certificato qualificato di firma elettronica:
a) in caso di temporanea sospensione di un certificato qualificato di firma elettronica, il certificato perde la sua validità per il periodo della sospensione;
b) il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato […]".

CAPITOLO 2: LA VALIDAZIONE TEMPORALE ELETTRONICA

2.1 INTRODUZIONE

In base a quanto analizzato nel precedente capitolo, il documento informatico ha la stessa valenza probatoria di una scrittura privata quando: sottoscritto mediante firma elettronica avanzata, qualificata o quando la sottoscrizione è in grado di identificare univocamente il firmatario e vengono rispettati sia i requisiti fissati dall'AgID, che i requisiti oggettivi del documento. Qualora, invece, il documento informatico fosse sprovvisto di firma elettronica o la sottoscrizione fosse avvenuta mediante firma elettronica semplice allora, sarà il giudice che, mediante il suo prudente apprezzamento, deciderà tenendo conto delle caratteristiche oggettive del documento. Tuttavia, anche un documento provvisto di firma elettronica avanzata o qualificata può essere oggetto del prudente apprezzamento da parte del giudice, quando disconosciuto dalla persona contro il quale è prodotto in giudizio ([69]).

Se ad un documento elettronico vengono riconosciuti determinati effetti giuridici è, anche, necessario che questi vengano mantenuti nel tempo e per fare ciò è necessaria una adeguata conservazione digitale.

La conservazione digitale è il procedimento informatico in grado di "conservare" i documenti elettronici in modo tale che i dati in essi contenuti non vengano modificati ([70]).

Sul tema si è soffermata in particolar modo l'Agenzia per l'Italia Digitale (AgID) che mediante la pubblicazione delle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* nel maggio 2021 si è prefissata di provvedere in maniera esaustiva ([71]).

---

[69] In tema di validità giuridica del documento informatico: DELFINI e FINOCCHIARO, *Diritto dell'informatica,* cit., p. 314.

[70] Considerando- 61: "*È opportuno che il presente regolamento garantisca la conservazione a lungo termine delle informazioni, al fine di assicurare la validità giuridica delle firme elettroniche e dei sigilli elettronici nel lungo periodo, garantendo che possano essere convalidati indipendentemente da futuri mutamenti tecnologici".*

[71] L'AgID in quanto autorità di vigilanza pubblica ha lo scopo di coordinare, tra le diverse attività, anche quelle inerenti al settore dell'e-governament, ossia l'utilizzo delle tecnologie informatiche nell'amministrazione pubblica ma ha anche il dovere di promulgare le linee guida e le regole tecniche per l'attuazione del Regolamento eIDAS. A questo proposito sono rilevanti le Linee guida pubblicate nel maggio 2021 in merito alla conservazione dei documenti informatici per far sì che il riferimento temporale possa essere valido. Il capitolo 4 è dedicato interamente alla conservazione dei documenti informatici, ove tra le diverse cose, si prevede l'obbligo per le pubbliche amministrazioni, i gestori di servizi pubblici, le società a controllo pubblico e i privati, ove non diversamente previsto dalla legge; di adottare un sistema di

Di fronte alla necessità per i soggetti pubblici e privati di ottenere con sufficiente certezza informazioni circa il momento di creazione del documento, di apposizione in esso della firma elettronica ([72]) o comunque di appurare l'esistenza di un determinato documento in un dato momento, la validazione temporale si è rivelata lo strumento idoneo a garantire data e ora certi, anche nei confronti dei terzi ([73]).

La validazione temporale elettronica è un servizio offerto da un prestatore di servizi in grado di associare ad un documento elettronico, data e ora, legalmente certi.

2.2 ELECTRONIC TIME STAMP

La disciplina dell'*electronic time stamp* ossia della validazione temporale elettronica ([74]), è prevista a livello comunitario, dal Regolamento eIDAS e completata, poi, a livello

conservazione a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti.
Il fine di questi sistemi di conservazione è quello di garantire l'accesso all'oggetto conservato per il periodo previsto. Inoltre, è lasciata alle Pubbliche Amministrazione la scelta di compiere la conservazione all'interno o all'esterno della struttura organizzativa dell'ente. Ancora, è obbligatorio per l'ente avere un manuale di conservazione, ossia di un documento informatico che deve illustrare in modo dettagliato, tra le tante cose, i soggetti coinvolti nel procedimento di conservazione, la descrizione delle architetture e delle infrastrutture utilizzate.

[72] I certificati di firma delle firme elettroniche sono soggetti a scadenza. Un certificato di firma dura tre anni per questo motivo è necessario applicare una marca temporale prima della scadenza dello stesso. L'unico fine è quello di garantire che la marca temprarle e perciò l'opponibilità del documento nei confronti delle parti e dei terzi fosse applicata e perciò in grado di dimostrare la validità della firma, prima della scadenza del certificato stesso.

[73] Prima di passare all'analisi della validazione temporale elettronica si ritiene utile, a titolo di completezza, ricordare che questo processo è importante anche in un'ottica di conservazione dei documenti informatici; infatti, anche la validazione temporale come i certificati di firma elettronica o altri metadati contenuti nei documenti informatici devono essere conservati in maniera adeguata affinché venga garantita la loro integrità. La conservazione digitale prevista anche dalla normativa nazionale (art. 43, 44, 44-*bis* cad) è importante in un'ottica di salvaguardia dei documenti informatici in modo tale che questi possano essere consultati e che la loro conservazione sia conforme agli originali e alle linee guida pubblicate da AgID. In particolare il d.p.c.m del 3 dicembre 2013 in materia di "*Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5 -bis , 23 -ter , comma 4, 43, commi 1 e 3, 44 , 44 -bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005"* introduce il concetto di "sistema di conservazione" all'art. 3 dove, riassumendo, si ribadisce la necessità di adoperare adeguati sistemi di conservazione, sia per la pubbliche amministrazione che per i soggetti privati, in modo tale da garantire un adeguato livello di certezza circa l'immodificabilità dei dati contenuti nei documenti. Rif: IASELLI, *Diritto e nuove tecnologie,* Milano, 2016, p.294.

[74] Al fine di fornire una quanto più completa analisi circa il tema della validazione temporale elettronica preme specificare che i termini marca temporale, riferimento temporale ed evidenza informatica, sono spesso utilizzati come sinonimi ma portano con sé delle specifiche differenti.
Cfr. IASELLI, *Diritto e nuove tecnologie,* cit., p.295*,* specifica che la validazione temporale elettronica è il risultato di una procedura informatica il cui fine è quello di attribuire data certa ed un orario, opponibili ai terzi, ad uno o più documenti informatici.
Cfr. art. 1 lett. i. e lett. m del d.p.c.m. 13.01.2004 prevede che: *"i) marca temporale: il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo;*
m) riferimento temporale: evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici".

nazionale sia dal Codice dell'Amministrazione Digitale che da diversi decreti del Presidente del Consiglio dei Ministri ([75]).

In base a quanto previsto a livello comunitario la validazione temporale elettronica può essere non qualificata ovvero qualificata.

La validazione temporale elettronica semplice è disciplinata all'art.3 n. 33 del Regolamento eIDAS ([76]) ed è il risultato di un procedimento informatico basato su una connessione di dati, il cui fine è quello di dimostrare che un dato documento esisteva ad una particolare data e ora.

Diversamente la validazione temporale qualificata, disciplinata al successivo punto n. 34 del cit. art., deve rispettare determinate prerogative per essere definita tale. I tre requisiti da soddisfare sono contenuti all'art. 42 del Reg. eIDAS e mirano a garantire un elevato livello di sicurezza in merito all'apposizione della data e dell'ora ([77]). Si tratta di tre requisiti cumulativi, vale a dire che devono sussistere tutti affinché la validazione

---

Cfr. all'art. 1 lett. f. del d.p.c.m. del 13.11.2014 stabilisce che l'evidenza informatica corrisponde ad *"una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica".*
Per tutto ciò se ne ricava che i termini validazione temporale e marca temporale sono gli strumenti tramite i quali è possibile attribuire una data ed un orario certi ad un documento. Mentre, il riferimento temporale, espresso mediante una sequenza di *bit*, corrisponde alla mera informazione contente la data e l'ora associata al documento informatico.

[75] Tra i principiali si riportano i d.p.c.m. del 22.02.2013, con pubblicazione in Gazzetta Ufficiale n. 117 il 21.05.2013 rubricato *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71.";* il d.p.c.m. del 13 novembre 2014, con pubblicazione in Gazzetta Ufficiale n. 8 il 12.01.2015 rubricato *"Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n.82 del 2005" e* infine quello del 13 gennaio 2004 *"Regole tecniche per la formazione, la trasmissione, la conversazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici",* con particolare riferimento al Titolo IV in materia di *"regole per la validazione temporale e per la protezione dei documenti informatici".*

[76] *"«validazione temporale elettronica», dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento".*

[77] *"1. Una validazione temporale elettronica qualificata soddisfa i requisiti seguenti:*
a) collega la data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati;
b) si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato; e
c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente".
2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili al collegamento della data e dell'ora ai dati e a fonti accurate di misurazione del tempo. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il collegamento della data e dell'ora ai dati e alla fonte accurata di misurazione del tempo rispondano a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2".

temporale si possa considerare come qualificata: qualora mancasse anche uno solo di questi elementi la validazione temporale non potrà essere inquadrata come qualificata.

Quanto al primo requisito, la lett. a) della disposizione citata esige che il *time stamp* colleghi i dati in modo da evitare la modifica di dati non rilevabili. Si tratta di un criterio non assoluto, ma piuttosto valutabile in relazione alla necessità di assicurare un elevato grado di sicurezza ed evitare le modifiche non riscontrabili dei dati connessi alla validazione. In altre parole, la valutazione, che deve essere fatta rispetto alla modificabilità dei dati, non deve essere rigida ma piuttosto dovrebbe essere segnata dal rispetto del principio della ragionevolezza ([78]). Principio per il quale la valutazione sarà soppesata, di volta in volta, anche rispetto alle tecnologie utilizzate.

La lett. b) richiede che la fonte di misurazione temporale sia accurata e collegata ad un sistema di tempo universale coordinato ([79]).

Quanto al terzo requisito, la possibilità di ottenere una validazione temporale elettronica può avvenire mediante apposizione di una firma elettronica qualificata oppure mediante un sigillo elettronico avanzato ([80]). Inoltre, il dettato normativo, tra le possibilità idonee

---

[78] Per comprendere meglio cosa si intenda con "principio della ragionevolezza" si rimanda all'art. 3 della Costituzione Italiana, dove si prevede che "*Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali.*
È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese".
Dal dettato normativo si comprende sicuramente la vigenza del principio di uguaglianza dal quale si ricava quello di ragionevolezza. In base a quest'ultimo principio le diposizioni normative devono essere congruenti rispetto al fine del legislatore. Va da sé, che nel caso in esame, considerare tutte le modifiche dei dati avvenute all'interno di un documento informatico, risulterebbe esagerato in quanto in contrasto con il fine del Regolamento eIDAS. Infatti, se il fine è, anche, quello di sviluppare un mercato unico digitale allora sarà necessario che il giudice valuti di volta in volta l'aspetto della modificabilità dei dati in relazione alle tecnologie impiegate.

[79] La necessità di individuare una *misurazione del tempo collegata al tempo universale coordinato,* è rappresentata dallo standard internazionale dell'UTC, *Coordinated Universal Time.* Si tratta di un sistema assunto come riferimento dalla moltitudine. Questo modello corrisponde all'ora media di Greenwich e rappresenta il punto di partenza dal quale misurare gli altri fusi orario del mondo. Ad esempio, per misurare il tempo nell'Europa Centrale, acronimo utilizzato CET, si scriverà UTC+1 vale a dire che l'orario in questa zona sarà di un'ora in più rispetto a Greenwich quando in vigore l'ora solare.

[80] Il sigillo elettronico è lo strumento che serve per autenticare i documenti elettronici appartenenti ad una persona giuridica. Il sigillo elettronico può essere semplice, avanzato ovvero qualificato. Nel caso in esame il sigillo elettronico avanzato è parificato ad una firma elettronica qualificata per le caratteristiche che entrambi sono in grado di garantire. Il sigillo elettronico avanzato di una persona giuridica è connesso unicamente al creatore del sigillo ed è in grado di identificarla. Inoltre, è creato mediante dati che sono in grado di identificare ogni successiva modifica e permette a colui che usufruisce di tale servizio il controllo, mediante un elevato livello di sicurezza del sigillo stesso. Il fondamento normativo che disciplina i requisiti che un sigillo elettronico avanzato deve sodisfare è l'art. 36 del Regolamento eIDAS. Invece il sigillo elettronico qualificato è semplicemente un sigillo elettronico avanzato (perciò avente gli stessi requisiti) e creato utilizzando un dispositivo dotato di certificato qualificato.

ad apporre un *qualified time stamp* menziona anche dei metodi equivalenti. Quest'ultimi sono i metodi "futuribili", che potranno emergere con il progresso tecnologico. Affinché il loro utilizzo conduca a ritenere apposta una validazione temporale elettronica qualificata, essi devono essere oggetto di verifica da parte del prestatore di servizi fiduciari che ne attesterà la capacità di garantire un livello di sicurezza equivalente, a quello garantito da un sigillo elettronico avanzato o da una firma elettronica avanzata, e un rispetto dei requisiti del Regolamento ([81]).

Il completamento di questa disciplina a livello nazionale è contenuto sia nel Codice dell'Amministrazione Digitale che nelle disposizioni contenute nelle regole tecniche emanante nei d.p.c.m. del 22 febbraio 2013 e del 13 novembre 2014.

Come emerge dal Titolo IV del primo di questi due decreti, recante le "*Regole per la validazione temporale mediante marca temporale*", il sistema italiano non riconosce, a differenza di quello europeo, due tipologie di validazione temporale elettronica bensì solo una ossia quella qualificata.

A questo fine, si chiarisce che se a livello italiano l'unica validazione temporale elettronica riconosciuta è quella qualificata, si individuano anche, altri metodi in grado di dimostrare la certezza della data (v. par. seguente).

Dalla lettura dell'art. 49 delle regole si ricava in maniera inequivoca che la validazione temporale elettronica deriva dall'utilizzo di chiavi di marcatura. È evidente qui il riferimento alla tecnica di crittografia utilizzata: quella asimmetrica. Ancora una volta si tratta di un sistema a chiave pubblica (come quello già visto per la firma forte, v. par. 1.4.3.2.) in grado di garantire un elevato livello di sicurezza (v. capitolo successivo). È appunto proprio per l'utilizzo di tale tecnica che la validazione temporale elettronica può essere considerata qualificata.

[81] Considerando 62: "*Al fine di garantire la sicurezza della validazione temporale elettronica qualificata, il presente regolamento dovrebbe richiedere l'uso di un sigillo elettronico avanzato o di una firma elettronica avanzata o di altri metodi equivalenti. È prevedibile che l'innovazione produca nuove tecnologie in grado di assicurare alla validazione temporale un livello di sicurezza equivalente. Ogni qualvolta venga utilizzato un metodo diverso dal sigillo elettronico avanzato o dalla firma elettronica avanzata, dovrebbe spettare al prestatore di servizi fiduciari qualificato dimostrare, nella relazione di valutazione di conformità, che tale metodo garantisce un livello equivalente di sicurezza e soddisfa gli obblighi previsti nel presente regolamento".*

2.3 ALTRI TIPI DI RIFERIMENTO TEMPORALE: analisi art. 41 d.p.c.m. 22 febbraio 2013.

Tuttavia, esistono altre tecniche, oltre alla validazione temporale elettronica, in grado di garantire con certezza il momento di formazione di un documento informatico.

Questi metodi, che di seguito andremo ad analizzare, sono regolamentati all'art. 41 co.4 del d.p.c.m. del 22.02.2013 ([82]).

In primo luogo, si considera valida ad accertare il riferimento temporale la segnatura di protocollo del sistema di gestione del flusso della pubblica amministrazione o dell'ente privato ([83]). La segnatura di protocollo consistente nell'apposizione, all'originale del documento, delle informazioni riguardanti lo stesso, come il codice identificativo dell'amministrazione e dell'area organizzativa omogenea, la data e il progressivo del protocollo. Oltre a queste specifiche informazioni, devono essere contenuti anche ulteriori dati quali quelli inerenti all'oggetto, al mittente e al destinatario.

Oppure, come previsto dal punto *b* della norma in esame, il riferimento temporale può essere garantito se la procedura di conservazione dei documenti avviene in conformità delle norme vigenti ([84]).

Infine, si considerano riferimenti temporali anche quelli ottenuti mediante l'utilizzo della Posta Elettronica Certificata e mediante marcatura postale elettronica.

La Posta Elettronica Certificata, più comunemente nota con l'abbreviazione di PEC, è un sistema di comunicazione elettronica che consente di inviare una mail con valore legale

---

[82] *"Costituiscono inoltre validazione temporale:*
a) il riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del decreto del Presidente del Consiglio dei Ministri, 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272;
b) il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una pubblica amministrazione;
c) il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata ai sensi dell'art. 48 del Codice;
d) il riferimento temporale ottenuto attraverso l'utilizzo della marcatura postale elettronica ai sensi dell'art. 14, comma 1, punto 1.4 della Convenzione postale universale, come modificata dalle decisioni adotta- te dal XXIII Congresso dell'Unione postale universale, recepite dal Regolamento di esecuzione emanato con il decreto del Presidente della Repubblica 12 gennaio 2007, n. 18."

[83] Per la definizione il rimando è al Decreto del presidente della Repubblica (d.p.r) n.445 del 2000 in materia di documentazione amministrativa dove all'art. 1 lett. s si prevede che: "*SEGNATURA DI PROTOCOLLO l'apposizione o l'associazione, all'originale del documento, in forma permanente e non modificabile delle informazioni riguardanti il documento stesso*".

[84] V. nota 73 in riferimento alle Linee guida pubblicate da AgID per la conservazione dei documenti digitali.

in quanto, grazie alle certificazioni previste, è in grado di assicurare un elevato livello di sicurezza ([85]).

Quanto all'ultimo riferimento temporale in grado di assicurare data certa ad un documento informatico, questo è rappresentato dalla marcatura postale elettronica. Si tratta del servizio offerto dagli operatori postali, come Poste Italiane S.p.A., il cui fine è quello di attestare che un evento elettronico è avvenuto in un determinato momento e in una data forma ([86]). Si tratta perciò dell'apposizione di una marca temporale in grado di data e ora, certe e legalmente valide.

In base a quanto fin qui detto, il riferimento temporale può essere garantito, non solo mediante il processo di validazione temporale elettronica, ma anche nelle forme previste dall'art.41 d.p.c.m. 2013 appena analizzato.

Tuttavia, il metodo più utilizzato per garantire con certezza la formazione di un documento informatico in un determinato momento è quello della validazione temporale, non solo per le sue caratteristiche intrinseche, ma anche per il suo riconoscimento giuridico negli altri Paesi dell'Unione. Infatti, come previsto dall'art. 41 Reg. cit. co. 3 "*Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri".*

---

[85] In rif. ROBOTTI, *La PEC- posta elettronica certificata,* in IASELLI, *Diritto e nuove tecnologie*, cit., p.321 ss. dove spiega la posta elettronica certificata.
Questa è comparata alla raccomandata cartaceo come la posta elettronica semplice (la c.d. mail) è paragonata alla lettera ordinaria. Spiega come la garanzia della PEC sia parificata a quella della raccomandata dato il sistema di certificazioni che sta alla base della prima. In poche parole, come nella raccomandata viene garantito l'arrivo e la consegna della stessa, anche nella PEC c'è un meccanismo molto simile. Questa tipologia di mail certificata si basa su un sistema di certificazioni. Il mittente, dopo aver effettuato tutti i vari controlli come il procedimento di identificazione, provvede alla scrittura del messaggio. Prima che quest'ultimo venga inviato passerà all'Internet Service Provider (ISP), che emetterà una ricevuta di accettazione corrispondente alla presa in carico del messaggio spedito. Successivamente, dopo che il gestore mittente invia la busta al gestore destinatario e dopo che sono stati messi in atto tutti i procedimenti appropriati per garantire l'inalterabilità del messaggio; arriverà al mittente una ricevuta di consegna, che attesta l'avvenuta disponibilità del messaggio presso il destinatario. In un'ottica di confronto tra la posta elettronica certificata e una raccomandata è preferibile la prima in termini di economicità in quanto un abbonamento annuale alla PEC è più conveniente rispetto all'invio di tante singole raccomandate e inoltre è uno strumento più flessibile perché l'invio della pec può avvenire in qualsiasi luogo.
V. anche art. 48 cad rubricato "*posta elettronica certificata*" e in particolare il co. 3 dove si disciplina che la data e l'ora di un documento informatico trasmessi mediante poste elettronica certificata sono opponibili ai terzi se conformi al Regolamento per l'utilizzo della stessa (d.p.r. n.68 del 2005) e alle relative regole tecniche.
[86] In base all'art. 1, lett. a) del d.p.c.m. del 14.12.2010, in materia di modalità tecnologiche di sicurezza e certificazione la marca postale elettronica è "*il servizio fornito dagli operatori postali che attesta in maniera probante la realta' di un evento elettronico sotto una data forma, in un certo momento ed al quale hanno partecipato una o piu' parti".*

2.4 I PRESTATORI DI SERVIZI FIDUCIARI:

In base a quanto previsto dal Regolamento eIDAS, quello che si viene a creare tra i soggetti che operano in questo ambito è un rapporto trilaterale dove agiscono:

- gli organismi di vigilanza pubblica, nella loro attività di controllo e tra i quali si ricorda per l'Italia AgID;
- le persone fisiche o giuridiche che invece usufruiscono dei servizi digitali offerti;
- e i prestatori di servizi fiduciari, in inglese *trust service provider*.

Il compito dei prestatori di servizi fiduciari è, oltre a quello di fornire i servizi fiduciari come quello di apposizione della firma elettronica o della validazione temporale ([87]), quello di garantire l'integrità e la correttezza di detti sistemi di identificazione mediante l'utilizzo di tecniche tecnologiche *ad hoc*.

Prima di analizzare i *trust service provider* è utile evidenziare che il Regolamento cit. non si applica a tutti prestatori di servizi bensì solamente a quelli aperti al pubblico e che offrono servizi aventi ripercussioni sui terzi ([88]).

---

[87] In merito ai servizi che un prestatore di servizi fiduciari può fare occorre fare un'ulteriore precisazione. Se con la Direttiva 1999/97/ce i prestatori di servizi fiduciari potevano compiere solamente attività di certificazione e altri servizi connessi alle firme elettroniche; ora con il Regolamento eIDAS la situazione è differente. Un prestatore di servizi, per quanto previsto dal Reg. cit. non compirà solamente attività di certificazione ma anche di creazione, verifica, convalida e conservazione della firma. Invece a livello nazionale, la possibilità per tsp di compiere diverse attività con l'unica differenza che se nella prima versione ì, d.lgs. 82 del 2005, il termine utilizzato era quello di "certificatori accreditati", ora, con le successive modifiche apportate dal d.lgs. 179 del 2016, il termine "accreditamento" è stato sostituito con quello di "qualificato". Rif. DELFINI e FINOCCHIARO, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, cit., p.49.

[88] Le indicazioni circa l'ambito di applicazione del Regolamento ai prestatori di servizi fiduciari sono riportate al C-21 dove si escludono coloro che offrono un servizio nell'ambito di un sistema chiuso e dove il servizio non ha alcuna ripercussione sui terzi.
C-21: "*È anche opportuno che il presente regolamento istituisca un quadro giuridico generale per l'impiego dei servizi fiduciari. Tuttavia, non è opportuno che istituisca un obbligo generale di farne uso o che installi un punto di accesso per tutti i servizi fiduciari esistenti. In particolare, non è auspicabile che il regolamento copra la prestazione di servizi fiduciari usati esclusivamente nell'ambito di sistemi chiusi da un insieme definito di partecipanti che non hanno ripercussioni su terzi. Ad esempio, i sistemi istituiti in imprese o amministrazioni pubbliche per la gestione delle procedure interne che fanno uso di servizi fiduciari non dovrebbero essere soggetti ai requisiti previsti dal presente regolamento. Solo i servizi fiduciari prestati al pubblico aventi ripercussioni su terzi dovrebbero soddisfare i requisiti previsti dal presente regolamento. Non è neanche auspicabile che il presente regolamento copra aspetti legati alla conclusione e alla validità di contratti o di altri vincoli giuridici nei casi in cui la normativa nazionale o unionale stabilisca obblighi quanto alla forma. Inoltre, non dovrebbe avere ripercussioni sugli obblighi di forma nazionali relativi ai registri pubblici, in particolare i registri commerciali e catastali*".
A mero titolo di completezza e sempre con riferimento ai prestatori di servizi fiduciari, il Reg. cit. prevede all'art.34 la possibilità anche per le persone fisiche di ricoprire il ruolo di conservazione di firme elettroniche qualificate. Questa precisazione viene fatta, perché se in un primo momento la normativa italiana negava alla figura del notaio la possibilità di compiere questa funzione di prestatori di servizi fiduciari, ora, con la determinazione n.629 del 2021 di AgID, ci si è uniformati al Reg. e perciò anche un

2.4.1 CLASSIFICAZIONE:

I *trust service provider (TSP*) sono soggetti, persone fisiche o giuridiche, il cui fine è quello di prestare un servizio fiduciario dietro remunerazione. La prestazione di tale servizio non è esclusiva, vale a dire che un prestatore (di servizi fiduciari), oltre a dimostrare l'esistenza di un documento in un determinato momento; può compiere ulteriori attività come quelle di verifica e convalida di firme elettroniche o ancora di conservazione di firme. Quanto appena spiegato è previsto all'art.3 n.16 del Regolamento ([89]).

Le tipologie di prestatori di servizi fiduciari previste dalla normativa europea sono due: prestatori non qualificati e qualificati.

Il primo è scarsamente disciplinato dalla normativa e semplicemente viene definito come un servizio fornito dietro remunerazione e chiaramente non esclusivo, vale a dire che sono diverse le attività che un soggetto può compiere ([90]).

Quanto alla seconda tipologia di servizi fiduciari disciplinata dal Regolamento cit. ossia quella di un *qualified trust service provider (QTSP)*, è stata ampiamente analizzata.

Innanzitutto, preme specificare che un servizio fiduciario è qualificato solo qualora, in base anche a quanto previsto dall'art. 3 n.17, siano rispettati i requisiti fissati dal Regolamento ([91]).

---

notaio potrà compiere la funzione di conservazione di documenti informatici. Rif: GENGHINI, *La forma notarile digitale*, Milano, 2022, p.207.

[89] "*«servizio fiduciario», un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:*
a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, servizi elettronici di recapito certificato e certificati relativi a tali servizi; oppure
b) creazione, verifica e convalida di certificati di autenticazione di siti web; o
c) conservazione di firme, sigilli o certificati elettronici relativi a tali servizi".

[90] V. nota precedente.

[91] Ex art. 24: *"1. Allorché rilascia un certificato qualificato per un servizio fiduciario, un prestatore di servizi fiduciari qualificato verifica, mediante mezzi appropriati e conformemente al diritto nazionale, l'identità e, se del caso, eventuali attributi specifici della persona fisica o giuridica a cui il certificato qualificato è rilasciato.*
Le informazioni di cui al primo comma sono verificate dal prestatore di servizi fiduciari qualificato direttamente o ricorrendo a un terzo conformemente al diritto nazionale:
2. Un prestatore di servizi fiduciari qualificato che presta servizi fiduciari qualificati:
a) informa l'organismo di vigilanza di eventuali cambiamenti nella prestazione dei propri servizi fiduciari qualificati e dell'intenzione di cessare tali attività;
b) impiega personale e, ove applicabile, subcontraenti dotati delle competenze, dell'affidabilità, dell'esperienza e delle qualifiche necessarie e che hanno ricevuto una formazione adeguata in materia di norme di sicurezza e di protezione dei dati personali e applica procedure amministrative e gestionali, che corrispondono a norme europee o internazionali;

Ciò che contraddistingue un *QTSP* da un prestatore (di servizi fiduciari) non qualificato è la capacità, del primo, di assicurare maggiori garanzie in merito ad affidabilità, trasparenza e sicurezza. Per fare ciò utilizza adeguati sistemi informatici idonei a garantire la memorizzazione in maniera stabile e duratura dei dati informatici e mediante l'utilizzo di appropriate procedure tecnologiche che prevengono da alterazioni o modificazioni i dati conservati.

Far parte della categoria *de qua* è un valore aggiunto per il prestatore stesso in un'ottica economica, in quanto si presenterà nel mercato come più affidabile rispetto ad un prestatore di servizi non qualificato. Ma d'altro canto rientrare in questa tipologia di prestatori implica delle responsabilità maggiori, come si vedrà nel prosieguo.

Il procedimento da seguire per l'avviamento di un servizio fiduciario qualificato non è immediato e presuppone varie fasi come disciplinato all'art. 21 del Regolamento cit. ([92]).

c) riguardo alla responsabilità civile per danni a norma dell'articolo 13, mantiene risorse finanziarie adeguate e/o si procura un'assicurazione di responsabilità civile appropriata, conformemente al diritto nazionale;
d) prima di avviare una relazione contrattuale informa, in modo chiaro e completo, chiunque intenda utilizzare un servizio fiduciario qualificato dei termini e delle condizioni esatte per l'utilizzo di tale servizio, comprese eventuali limitazioni del suo utilizzo;
e) utilizza sistemi affidabili e prodotti protetti da alterazioni e che garantiscono la sicurezza tecnica e l'affidabilità dei processi che assicurano;
f) utilizza sistemi affidabili per memorizzare i dati a esso forniti, in modo verificabile, affinché:
i) siano accessibili alla consultazione del pubblico soltanto con il consenso della persona a cui i dati fanno riferimento;
ii) soltanto le persone autorizzate possano effettuare inserimenti e modifiche ai dati memorizzati;
iii) l'autenticità dei dati sia verificabile;
g) adotta misure adeguate contro le falsificazioni e i furti di dati;
h) registra e mantiene accessibili per un congruo periodo di tempo, anche dopo la cessazione delle attività del prestatore di servizi fiduciari qualificato, tutte le informazioni pertinenti relative a dati rilasciati e ricevuti dal prestatore di servizi fiduciari qualificato, in particolare a fini di produzione di prove nell'ambito di procedimenti giudiziali e per assicurare la continuità del servizio. Tali registrazioni possono essere elettroniche;
i) dispone di un piano di cessazione delle attività aggiornato per garantire la continuità del servizio conformemente alle disposizioni verificate dall'organismo di vigilanza a norma dell'articolo 17, paragrafo 4, lettera i);
j) garantisce il trattamento lecito dei dati personali a norma della direttiva 95/46/CE;
k) se i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati, istituiscono una banca dati dei certificati aggiornata. […]"

[92] *1. Qualora i prestatori di servizi fiduciari, privi di qualifica, intendano avviare la prestazione di servizi fiduciari qualificati, trasmettono all'organismo di vigilanza una notifica della loro intenzione insieme a una relazione di valutazione della conformità rilasciata da un organismo di valutazione della conformità.*
2. L'organismo di vigilanza verifica se il prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti di cui al presente regolamento e, in particolare, i requisiti per i prestatori di servizi fiduciari qualificati e per i servizi fiduciari qualificati da essi prestati.
Se conclude che il prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti di cui al primo comma, l'organismo di vigilanza concede la qualifica al prestatore di servizi fiduciari e ai servizi fiduciari da esso prestati e informa l'organismo di cui all'articolo 22, paragrafo 3, affinché aggiorni

Innanzitutto, il prestatore di servizi fiduciari che vuole erogare una prestazione qualificata deve notificare questa volontà ad un organismo di vigilanza con una relazione di valutazione della conformità. Se l'esito dell'attività di verifica da parte dell'organismo di vigilanza sarà positivo allora si procederà con l'iscrizione del servizio negli elenchi di fiducia, normati all'art. 22. Questi registri, contenenti tutte le informazioni relative ai prestatori di servizi fiduciari qualificati, sono essenziali per garantire un elevato livello di certezza tra gli operatori del mercato interno e sarà onere degli Stati membri redigerli, mantenerli e pubblicarli in un canale internet sicuro.

Ancora: ciò che contraddistingue i prestatori di servizi fiduciari qualificati da quelli non qualificati è la possibilità per i primi di avere un marchio di fiducia ([93]). Si tratta di un logo che garantisce la prestazione di un elevato livello di sicurezza da parte dei prestatori di servizi fiduciari ([94]).

---

gli elenchi di fiducia di cui all'articolo 22, paragrafo 1, non oltre tre mesi dopo la notifica a norma del paragrafo 1 del presente articolo.
Se la verifica non si è conclusa entro tre mesi dalla notifica, l'organismo di vigilanza ne informa il prestatore di servizi fiduciari specificando i motivi del ritardo e il periodo necessario per concludere la verifica.
3. I prestatori di servizi fiduciari qualificati possono iniziare a prestare il servizio fiduciario qualificato dopo che la qualifica è stata registrata negli elenchi di fiducia di cui all'articolo 22, paragrafo 1.
4. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure della relazione di cui ai paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2".

[93] Art. 23 Reg. eIDAS: *"1. Dopo la registrazione della qualifica di cui all'articolo 21, paragrafo 2, secondo comma, nell'elenco di fiducia di cui all'articolo 22, paragrafo 1, i prestatori di servizi fiduciari qualificati possono utilizzare il marchio di fiducia UE per presentare in modo semplice, riconoscibile e chiaro i servizi fiduciari qualificati da essi prestati.*
2. Quando utilizzano il marchio di fiducia UE per i servizi fiduciari qualificati di cui al paragrafo 1, i prestatori di servizi fiduciari qualificati garantiscono che sul loro sito web sia disponibile un link all'elenco di fiducia pertinente.
3. Entro il 1° luglio 2015 la Commissione, mediante atti di esecuzione, fornisce criteri specifici relativi alla forma e, in particolare, alla presentazione, alla composizione, alla dimensione e al disegno del marchio di fiducia UE per i servizi fiduciari qualificati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2."

[94] La Commissione mediante Regolamento di esecuzione (UE) 2015/806 ne stabilisce le specifiche. Il fine è chiaramente quello di innalzare il livello di fiducia che gli utenti finali possono avere nei confronti dei prestatori dotati di questo marchio e ancora facilitare l'uso dei loro servizi. Interessante è che per il design del nuovo luogo la Commissione abbia organizzato il concorso "E-Mark U Trust" affinché fossero gli studenti degli istituti d'arte e design a fare nuove proposte. Tuttavia, il Regolamento di esecuzione disciplina tra le diverse cose quali debbano essere i colori da utilizzare per il marchio di fiducia UE o ancora la grandezza dello stesso. in riferimento ai colori qualora si possano utilizzare allora questi devono essere Pantone 654 e 116 qualora invece questi non potessero utilizzati si farà riferimento al solo bianco e nero. In merito alla grandezza le dimensioni non potranno essere inferiori a 64x 85 pixel con risoluzione di 150 dpi.

2.4.2 ACCESSIBILITÀ DEI SERVIZI FIDUCIARI

In un'ottica di inclusività in relazione agli utenti finali che possono accedere ai servizi fiduciari offerti dai prestatori l'art. 15 del Regolamento cit. rubricato "*Accessibilità per le persone con disabilità*" stabilisce che i servizi fiduciari sono accessibili anche agli utenti finali con disabilità.

La normativa comunitaria si è uniformata alla normativa internazionale, in particolare all'art.9 della Convenzione delle Nazioni Unite per i diritti delle persone con disabilità ([95]), dove vengono elencate le misure che gli Stati Parti dovrebbero adottare per abbattere le barriere di accessibilità per gli utenti con disabilità.

Anche il legislatore nazionale è intervenuto sul tema dell'accessibilità: all'art. 8 CAD, rubricato "*Alfabetizzazione informatica dei cittadini"*, si esprime la necessità di promuovere iniziative che includano anche le categorie a rischio di esclusione, proprio come quelle in esame. In proposito, l'art. 17, lett. d) CAD prevede che ogni Pubblica Amministrazione debba garantire l'attuazione delle linee strategiche per la riorganizzazione e digitalizzazione delle amministrazioni in base a quanto stabilito dal Governo in conformità all'art. 71 co.1-ter CAD ([96]).

2.4.3 DAGLI ORGANISMI DI VIGILANZA AI COMPITI DEI PRESTATORI DI SERVIZI FIDUCIARI

All'attività di vigilanza dei prestatori di servizi fiduciari è dedicata l'intera Sezione II del capo III del Regolamento cit. ([97]).

---

[95] La Convenzione delle Nazioni Unite per i diritti delle persone con disabilità è stata adottata il 13 dicembre 2006 dall'Assemblea Generale dell'ONU. Con legge 3.03.2009 il Parlamento italiano ha autorizzato la rettifica della Convenzione e solo dopo, con il Consiglio 2010/48/CE, anche la Comunità Europea ha aderito alla Convezione. In particolare, si rimanda all'art. 9 rubricato "*Accessibilità"* della Convenzione internazionale dove si prevede che i soggetti con disabilità debbano essere in grado di accedere, anche, ai servizi dell'informazione sulla base del principio di uguaglianza con gli altri. Lo scopo è quello di *promuovere, proteggere e garantire* il pieno godimento delle libertà fondamentali e dei diritti umani da parte degli utenti con disabilità, per fare ciò sono diverse le misure adeguate ad adottare proposte. Per esempio, l'art.9 prevede la necessità di dotare le strutture e gli edifici aperti al pubblico della segnaletica tattile come quella Braille per gli utenti non vedenti in modo tale da abbattere le barriere di accessibilità a questi servizi. O ancora gli Stati parti dovrebbero promuovere forme adeguate di assistenza e sostengo a persone non autosufficienti per garantire loro l'accesso all'informazione o alle nuove tecnologie di comunicazione, compreso internet.

[96] "*1-ter. Le regole tecniche di cui al presente codice sono dettate in conformità ai requisiti tecnici di accessibilità di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, alle discipline risultanti dal processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea".*

[97] v. anche C-30 ss. reg. cit.

In particolare, l'art. 17 rubricato *"Organismo di vigilanza"* ([98]) disciplina l'intero regime di vigilanza che svolge un ruolo essenziale nell'assicurare sicurezza e attendibilità dei servizi prestati.

In base a quanto previsto dal par. 1 articolo in esame, ogni Stato membro dovrebbe nominare uno o più organismi di vigilanza per svolgere le attività di controllo previste dal

[98] "*1. Gli Stati membri designano un organismo di vigilanza stabilito nel loro territorio o, di comune accordo con un altro Stato membro, un organismo di vigilanza stabilito in tale altro Stato membro. Tale organismo è responsabile di compiti di vigilanza nello Stato membro designante.*
Agli organismi di vigilanza sono conferiti i poteri necessari e le risorse adeguate per l'esercizio dei loro compiti.
2. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi dei rispettivi organismi di vigilanza designati.
3. Il ruolo dell'organismo di vigilanza è il seguente:
a) vigilare sui prestatori di servizi fiduciari qualificati stabiliti nel territorio dello Stato membro designante per assicurarsi, mediante attività di vigilanza ex ante e ex post, che essi e i servizi fiduciari qualificati da essi prestati rispondano ai requisiti di cui al presente regolamento;
b) adottare misure, ove necessario, in relazione a prestatori di servizi fiduciari non qualificati stabiliti nel territorio dello Stato membro designante, mediante attività di vigilanza ex post, qualora sia informato che tali prestatori di servizi fiduciari non qualificati o i servizi fiduciari da essi prestati presumibilmente non soddisfano i requisiti stabiliti dal presente regolamento.
4. Ai fini del paragrafo 3 e fatte salve le limitazioni ivi previste, l'organismo di vigilanza ha, in particolare, i compiti seguenti:
a) cooperare con altri organismi di vigilanza e assisterli a norma dell'articolo 18;
b) analizzare le relazioni di valutazione della conformità di cui all'articolo 20, paragrafo 1, e all'articolo 21, paragrafo 1;
c) informare gli altri organismi di vigilanza e il pubblico in merito a violazioni della sicurezza o perdita di integrità a norma dell'articolo 19, paragrafo 2;
d) riferire alla Commissione in merito alle sue principali attività a norma del paragrafo 6 del presente articolo;
e) svolgere verifiche o chiedere a un organismo di valutazione della conformità di effettuare una valutazione di confor mità dei prestatori di servizi fiduciari qualificati a norma dell'articolo 20, paragrafo 2;
f) cooperare con le autorità di protezione, in particolare informandole senza indugio dei dati in merito ai risultati di verifiche di prestatori di servizi fiduciari qualificati, laddove siano state rilevate violazioni delle norme di protezione dei dati personali;
g) concedere la qualifica ai prestatori di servizi fiduciari e ai servizi da essi prestati e ritirare tale qualifica a norma degli articoli 20 e 21;
h) informare l'organismo responsabile dell'elenco nazionale di fiducia di cui all'articolo 22, paragrafo 3, in merito alle proprie decisioni di concedere o ritirare la qualifica, salvo se tale organismo è anche l'organismo di vigilanza;
i) verificare l'esistenza e la corretta applicazione delle disposizioni sui piani di cessazione nei casi in cui il prestatore di servizi fiduciari qualificati cessa le sue attività, inclusi i modi in cui le informazioni sono mantenute accessibili a norma dell'articolo 24, paragrafo 2, lettera h);
j) imporre ai prestatori di servizi fiduciari di rimediare a qualsiasi mancato adempimento dei requisiti di cui al presente regolamento.
5. Gli Stati membri possono imporre che l'organismo di vigilanza istituisca, mantenga e aggiorni un'infrastruttura fiduciaria secondo le condizioni di cui al diritto nazionale.
6. Entro il 31 marzo di ogni anno, ogni organismo di vigilanza presenta alla Commissione una relazione sulle sue principali attività del precedente anno civile insieme a una sintesi delle notifiche di violazione ricevute da prestatori di servizi fiduciari a norma dell'articolo 19, paragrafo 2.
7. La Commissione mette a disposizione degli Stati membri la relazione annuale di cui al paragrafo 6.
8. La Commissione può, mediante atti di esecuzione, definire i formati e le procedure della relazione di cui al paragrafo
9. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2".

Regolamento cit. Lo Stato membro può, tuttavia, nominare di comune accordo con un altro Stato membro, un organismo di vigilanza posto fuori dal suo territorio, ma comunque all'interno dell'Unione; l'organismo sarà responsabile per compiti di vigilanza nello Stato designante. Tale possibilità si rifà, ancora una volta, al principio dell'interoperabilità operante all'interno dell'Unione.

L'organismo di vigilanza nominato dall'Italia è AgID ([99]).

Infine, è previsto che gli organismi di vigilanza abbiano *i poteri necessari* e *le risorse adeguate* all'adempimento dei loro compiti.

Come previsto dal par. 2 sarà poi onere dei singoli Stati membri notificare alla Commissione i nomi e gli elenchi dei rispettivi organi di vigilanza.

Il par. 3 disciplina invece l'attività di controllo svolta dagli organismi di vigilanza sui prestatori di servizi fiduciari. Fin da subito è chiaro che l'attività di controllo è differente se è eseguita nei confronti di un prestatore di servizi fiduciari qualificati (lett. a) ovvero se è eseguito su un prestatore non qualificato (lett. b).

Nel primo caso il controllo verterà sui requisiti previsti dall'art. 21 del Regolamento (v. *supra*) e potrà verificarsi sia ex ante che ex post. Nel caso di un controllo ex ante lo scopo sarà quello di prevenire eventuali violazioni da parte del soggetto per cui è previsto il controllo, mentre un'attività ex post avviene nel momento in cui emergono criticità o violazioni, per esempio, nei criteri di sicurezza e attendibilità dei servizi prestati ([100]).

---

[99] In merito al ruolo centrale assunto da AgID a seguito dell'ultimo intervento normativo (d.lgs. n.179 del 2016 che integra e modifica il precedente d.lgs. n.82 del 2005, noto come cad) si è espresso anche il Consiglio di Stato, comm. spec.,n. 2122 del 10/10/2017: "*In ordine allo schema di decreto legislativo recante disposizioni integrative e correttive al decreto legislativo 26 agosto 2016, n. 179, concernente « modifiche e integrazioni al Codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'art. 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche », per il tramite delle novelle di cui all'intervento normativo in esame l'AgID ha assunto un ruolo centrale nella presente materia sia nell'ambito dei rapporti con la cittadinanza sia relativamente ai rapporti con le pubbliche amministrazioni. Pertanto, in considerazione di quanto precede, è auspicabile che l'Amministrazione effettui anche una valutazione dell'adeguatezza dell'attuale organizzazione di tale ente — a fronte delle rilevanti ed impegnative nuove funzioni che sono attribuite — procedendo agli opportuni cambiamenti qualora emerga che tale organizzazione non sia del tutto idonea ad assolvere ai complessi compiti assegnati*".

[100] Anche l'art. 20 del cit. Reg. disciplina il regime di vigilanza dei prestatori (di servizi fiduciari) qualificati. Viene anzitutto disciplinata l'attività di verifica che dovrà avvenire almeno ogni 24 mesi e a spese del prestatore. Tuttavia, l'organismo di vigilanza può avviare in un qualsiasi momento attività di verifica o di conformità sempre allo stesso fine ossia quello di verifica che i requisiti del Reg. vengano rispettati. Infine, è previsto che qualora un prestatore non rimedi agli obblighi dal Regolamento disattesi, l'organismo possa procedere con la revoca della qualifica del prestatore.

Tuttavia, l'attività di prestatore nei confronti di un servizio fiduciario qualificato non è assoggettata alla sola attività di controllo, ma, come previsto dalla stessa norma (par. 4 lett. e, lett. g), anche a quella di verifica e analisi della conformità dei prestatori.

Per i prestatori (di servizi fiduciari) non qualificati, l'attività di vigilanza è meno gravosa rispetto a quella appena analizzata. Essi non sono soggetti ad un generale obbligo di controllo, ma piuttosto ad un esclusivo controllo ex post che si verifica solo qualora vi sia la prova che il servizio fiduciario non rispetti i requisiti del Regolamento. Si tratta, perciò, di un controllo semplice e reattivo che si verifica solo *ove necessario* ([101]).

Detto tutto ciò e data la possibilità per i singoli Stati membri di individuare in modo autonomo l'organismo di vigilanza, si ricorda, tuttavia, che il ruolo centrale a livello europeo è quello della Commissione. Come previsto dal par. 6 annualmente tutti gli organismi devono informarla circa le attività condotte e sarà poi compito della Commissione redigere la redazione annuale (v. par. 6,7,8,). Considerando quanto appena ricordato, l'attività di cooperazione da parte degli organismi di vigilanza (nell'informare, per esempio, su eventuali violazioni dell'integrità dei dati) costituisce un obbligo generalizzato, nel senso che l'attività di collaborazione non è solo tra organismi di vigilanza, ma anche nei confronti della Commissione e degli utenti finali del servizio ([102]).

I prestatori di servizi fiduciari, oltre ad essere soggetti alle attività di vigilanza da parte degli organismi predetti, devono anche assolvere gli obblighi loro deputati in base alla

[101] Il rinvio è al C-36 del Reg. cit. dove è spiegato come dovrebbe essere il controllo effettuato da un organismo di viglanza nei confronti di un prestatore di servizi fiduciari: "*L'istituzione di un regime di vigilanza per tutti i prestatori di servizi fiduciari dovrebbe assicurare parità di condizioni per la sicurezza e l'attendibilità delle loro operazioni e servizi, contribuendo in tal modo alla tutela degli utenti e al funzionamento del mercato interno. I prestatori di servizi fiduciari non qualificati dovrebbero essere soggetti ad attività di vigilanza ex post semplificate e reattive, giustificate dalla natura dei loro servizi e delle loro operazioni. Pertanto l'organismo di sorveglianza non dovrebbe avere un obbligo generale di vigilanza sui prestatori di servizi non qualificati. L'organismo di sorveglianza dovrebbe adottare misure solo quando viene informato (ad esempio, dallo stesso prestatore di servizi fiduciari non qualificati, da un altro organismo di sorveglianza, mediante la notifica di un utente o di un partner commerciale o in base a sue indagine proprie) che un prestatore di servizi fiduciari non qualificato non soddisfa i requisiti del presente regolamento".*

[102] Non a caso la lett. a dell'articolo in commento rimanda all'art.18 rubricato "*assistenza reciproca*". Il tema è evidente e riguarda quello della stretta collaborazione che deve sussistere tra i differenti prestatori di servizi fiduciari. La richiesta di assistenza da parte di un organismo di vigilanza si traduce in una richiesta di aiuto ossia di affiancamento verso un altro prestatore. Perciò quest'ultimo non dovrà sostituirsi al prestatore che richiede aiuto. Inoltre, una richiesta di aiuto non potrà mai essere rifiutata ovvero negata a meno che non sussistono i tre casi tassativi per il legittimo rifiuto. la richiesta può essere rifiutata quando l'organismo non è competente fornire quanto richiesta oppure quando la prima è sproporzionata risetto a quanto previsto dal regolamento. Ultima ipotesi di rifiuto tassativo è quando, quanto richiesto potrebbe porsi in contrasto con la normativa. Rif: DELFINI e FINOCCHIARO, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, cit., p.179 ss. V. anche C-42 Regolamento eIDAS.

loro natura. L'art. 19 del Reg. cit. rubricato "*Requisiti di sicurezza relativi ai prestatori di servizi fiduciari"* ([103])*,* evidenzia due obblighi generali in capo al prestatore di servizi fiduciari. Il fine della norma in commento è quello di garantire un elevato livello di fiducia e affidamento dal lato utente; e dal lato prestatore stabilire adeguati modelli di trasparenza.

In primo luogo, l'obbligo generale di sicurezza deve essere garantito, tenendo conto dello sviluppo tecnologico e delle misure adottate ([104]).

Nel co. 2 del cit. art, è sancito l'obbligo di notifica all'organismo di vigilanza quando si verificano violazioni della sicurezza o la perdita di integrità dei dati personali. L'obbligo di notifica come previsto dal dettato normativo deve verificarsi solo quando si tratta di un *impatto significativo* sul servizio stesso o sui dati conservati. La previsione implica da parte del prestatore di servizi una grande opera di valutazione in merito alle violazioni verificatesi, in quanto una mancata notifica può comportare anche una responsabilità nei

---

[103] "*1. I prestatori di servizi fiduciari qualificati e non qualificati adottano le misure tecniche e organizzative appropriate per gestire i rischi legati alla sicurezza dei servizi fiduciari da essi prestati. Tenuto conto degli ultimi sviluppi tecnologici, tali misure assicurano un livello di sicurezza commisurato al grado di rischio esistente. In particolare, sono adottate misure per prevenire e minimizzare l'impatto degli incidenti di sicurezza e informare le parti interessate degli effetti negativi di eventuali incidenti.*
2. Senza indugio ma in ogni caso entro 24 ore dall'esserne venuti a conoscenza, i prestatori di servizi fiduciari qualificati e non qualificati notificano all'organismo di vigilanza e, ove applicabile, ad altri organismi interessati, quali l'ente nazionale competente per la sicurezza delle informazioni o l'autorità di protezione dei dati, tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi.
Qualora sia probabile che la violazione della sicurezza o la perdita di integrità abbia effetti negativi su una persona fisica o giuridica a cui è stato prestato il servizio fiduciario, il prestatore di servizi fiduciari notifica senza indugio anche alla persona fisica o giuridica la violazione di sicurezza o la perdita di integrità.
Ove appropriato, in particolare qualora la violazione di sicurezza o la perdita di integrità riguardi due o più Stati membri, l'organismo di vigilanza notificato ne informa gli organismi di vigilanza negli altri Stati membri interessati e l'ENISA.
L'organismo di vigilanza notificato informa il pubblico o impone al prestatore di servizi fiduciari di farlo, ove accerti che la divulgazione della violazione della sicurezza o della perdita di integrità sia nell'interesse pubblico.
3. L'organismo di vigilanza trasmette all'ENISA, una volta all'anno, una sintesi delle notifiche di violazione di sicurezza e perdita di integrità pervenute dai prestatori di servizi fiduciari.
4. La Commissione può, mediante atti di esecuzione:
a) specificare ulteriormente le misure di cui al paragrafo 1; e
b) definire i formati e le procedure, comprese le scadenze, applicabili ai fini del paragrafo 2.
Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2".

[104] Sono evidenti in questo caso le similitudini con la normativa in materia di protezione dei dati personali, il Regolamento UE n.679 del 2016 anche noto come *General Data Protection Regulation* e in particolare con l'art. 32. In questo articolo l'obbligo di sicurezza si declina, da una parte nell'obbligo da parte del titolare e del responsabile del trattamento tenuto conto dello sviluppo tecnologico, un livello di sicurezza adeguato al rischio proprio come previsto all'art. 19 co.1. E, all'art. 33 GDPR, un obbligo di notifica al verificarsi delle violazioni dei dati personali, ancora una volta come previsto dall'art.19 co.2. Rif: *DELFINI e FINOCCHIARO, Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. Commento al Regolamento UE 910/2014, cit., p.185.*

confronti del soggetto medesimo. Inoltre, l'atto di notificazione deve avvenire senza alcun ingiustificato ritardo e comunque entro 24 ore dall'avvenuta conoscenza da parte del prestatore.

La notifica non avviene solamente nei confronti dell'organismo di vigilanza, ma anche verso l'interessato stesso in modo tale che questo abbia la possibilità di prendere gli accorgimenti necessari.

Ancora, qualora le violazioni riguardassero due o più Stati membri, la notifica dovrà essere fatta sia nei confronti degli Stati interessati che nei confronti dell'*European union agency for cybersecurity* (ENISA) ([105]).

2.4.4 RESPONSABILITÀ

La responsabilità dei prestatori di servizi fiduciari è disciplinata all'art. 13 del Regolamento eIDAS, nel quale si prevede che: "*1. Fatto salvo il paragrafo 2, i prestatori di servizi fiduciari sono responsabili di danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito a un mancato adempimento degli obblighi di cui al presente regolamento.*
L'onere di dimostrare il dolo o la negligenza di un prestatore di servizi fiduciari non qualificato ricade sulla persona fisica o giuridica che denuncia il danno di cui al primo comma.
Si presume il dolo o la negligenza di un prestatore di servizi fiduciari qualificato, salvo se questi dimostra che il danno di cui al primo comma si è verificato senza suo dolo o negligenza.
2. Se i prestatori di servizi fiduciari informano debitamente e preventivamente i loro clienti delle limitazioni d'uso dei servizi da essi forniti e se tali limitazioni sono riconoscibili da parte di terzi, non sono responsabili dei danni che derivano dall'utilizzo di servizi oltre i limiti indicati".

La responsabilità *de qua* è prevista per i prestatori di servizi fiduciari nei confronti di *qualsiasi persona fisica o giuridica* e perciò rientrano nella formulazione anche i terzi, ossia coloro non sono legati ad un vincolo contrattuale con i prestatori, ma che possono subire i pregiudizi delle azioni di questi. Ad esempio, un prestatore che nell'operare, per esempio, un servizio fiduciario di conservazione dei documenti digitali arrechi un danno

[105] Si tratta di una agenzia dell'Unione europea il cui fine è quello di garantire la sicurezza digitale dei cittadini dell'UE.

nei confronti di un terzo dovrà preoccuparsi di risarcirlo qualora derivasse da suo presunto dolo o negligenza.

Quanto al par. 2 il presupposto è una responsabilità extracontrattuale. Il prestatore è responsabile anche nei confronti dei terzi. Invece, qualora fosse il soggetto stesso ad utilizzare il servizio offerto oltre i limiti d'uso, già resi conoscibili anche nei confronti dei terzi allora si escluderà qualsiasi responsabilità in capo al prestatore dei servizi fiduciari ([106]).

Quanto all'ultimo paragrafo l'interpretazione che sembra preferibile è quella secondo la quale il regime posto dalle norme interne viene mantenuto fino al momento in cui non sarà lo stesso Regolamento ad innovarlo mediante disposizioni *ad hoc*. Vale a dire che si mantengono le categorie di diritto interno fino a quando lo stesso Regolamento, in sede di revisione, non venga a prevedere delle disposizioni differenti, in questo caso allora lo scenario si riterrà innovato. A titolo esemplificativo, le categorie di diritto interno sono state rinnovate dal Regolamento, nel momento in cui è quest'ultimo a prevedere l'esclusione di responsabilità per i prestatori di servizi fiduciari quando il servizio viene utilizzato, dagli utenti finali, oltre i limiti d'uso, previamente specificati dagli stessi.

In quest'ottica il panorama tradizionale è stato deviato solo con riguardo al par. 1 dell'articolo, dove è stata introdotta una presunzione di dolo o negligenza nei confronti del prestatore di servizi fiduciari qualificato, il quale potrà esimersi da responsabilità fornendo una prova contraria. Con riguardo, invece, alla prima parte dell'articolo, la disciplina dell'onere della prova è la stessa che deriva dal diritto interno con particolare riferimento all'art. 2043 c.c. ([107]).

---

[106] Con riferimento alla disciplina sui limiti d'uso dei servizi fiduciari è importante il c-37 del Regolamento dove nella prima parte si ribadisce il regime di responsabilità dei servizi fiduciari. Tuttavia, nella seconda parte si stabilisce che, per questi soggetti, è possibile stabilire limiti all'uso di tali servizi. Dovranno poi procedere a informare debitamente e anticipatamente gli utenti finali e rendere le informazioni conoscibili anche per i terzi. Così facendo un prestatore di servizi fiduciari è escluso da responsabilità quando il cliente stesso supera i limiti d'utilizzo del servizio. Questo principio è stato recepito anche a livello nazionale dal Codice dell'Amministrazione Digitale dove all'art. 30. par.3 viene ribadito la stessa regola. E ancora all'art. 28 par.3 lett. b) dove si prevede che un certificato di firma elettronica debba contenere, tra le altre informazioni, anche quella circa i limiti d'uso del certificato. Rif: DELFINI e FINOCCHIARO, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, cit., p.154.

[107] L'art. 2043 c.c. costituisce il fondamento della responsabilità extracontrattuale o aquiliana per la quale l'autore di una lesione di un diritto di un altro soggetto dovrà necessariamente procedere con il risarcimento per i danni negativi patrimoniali e non. In merito al concetto di danno, la dottrina e la giurisprudenza hanno dibattuto per molto tempo e quello che è emerso è che il danno ingiusto risarcibile è sia quello patrimoniale che non patrimoniale vale a dire che la non patrimonialità non è elemento di esclusione al risarcimento del danno. Attenzione che i casi di risarcimento sono esclusivamente quelli previsti dalla legge *ex* art. 2059 c.c. (*ex multis* Trib. Milano n.3867 del 2023). Con riferimento al *fatto doloso o colposo* si fa riferimento nel

2.4.5 SANZIONI

I prestatori di servizi fiduciari che violano il Regolamento eIDAS sono soggetti a sanzioni che come previsto dall'art. 16 ([108]) della normativa in esame, devono essere "*effettive*", "*proporzionate*" e "*dissuasive*".

È evidente che il dettato normativo sia molto generico e che non entri nel dettaglio delle sanzioni da applicare. Pertanto, viene lasciato un certo margine di discrezionalità a ciascun Stato membro nell'irrogare le dovute sanzioni.

Preme tuttavia ricordare che esistono regole di coordinamento atte a regolare le misure che gli Stati possono impiegare. In altre parole, le Istituzioni dell'Unione impongono agli Stati membri obblighi di risultato vincolanti, che necessitano poi di un piano di armonizzazione a livello nazionale. Se a livello comunitario il Regolamento eIDAS ha come fine quello di stabilire una disciplina generale in materia di strumenti informatici e telematici, è il legislatore nazionale che si deve occupare di attuare un adeguato piano di armonizzazione. Esempio a livello nazionale di questo piano di armonizzazione è proprio il CAD ([109]).

Un altro importante principio comunitario è quello della leale collaborazione, il quale indica che gli Stati membri devono assicurare l'esecuzione degli obblighi derivanti dagli atti dell'Unione mediante l'adozione di misure nazionali ([110]).

---

caso del dolo alla definizione dell'art. 43 del c.p. e in particolare si evidenzia l'importanza dell'elemento soggettivo. Diversamente la definizione di colpa è più complessa, in quanto non vi è alcuna definizione nel Codice civile. Ad ogni modo si fa riferimento più comunemente al fatto che deriva da negligenza, imprudenza o imperizia di colui che provoca il danno. Rif: CIAN, TRABUCCHI, *Commentario al Codice civile*, cit., sub. Art. pag. 2236.

[108] "*Gli Stati membri stabiliscono norme relative alle sanzioni da applicare in caso di violazioni del presente regolamento. Le sanzioni previste sono effettive, proporzionate e dissuasive".*

[109] Con riferimento al piano di armonizzazione che ogni Stato membro deve attuare si ricorda che la disamina fin qui proposta si è infatti mossa su due livelli di analisi. Per esempio, rispetto alla definizione delle firme elettroniche si sono proposte quelle comunitarie dove, tra l'altro, nella maggior parte dei casi vige il principio della net neutralità, una sorta di "libertà tecnologica" per poi passare al piano nazionale dove invece le definizioni sono sempre più dettagliate.

[110] Il fondamento è l'art. 4 del Trattato sull'Unione Europea con particolare riferimento al par.3 dove si disciplina il principio della leale collaborazione. In base a questo principio l'Unione e ogni Stato membro si rispettano e si assistono reciprocamente nell'adempimento dei compiti derivanti dal Trattato. Nel caso in esame l'obbligo derivante dal Regolamento eIDAS è quello di stabilire un quadro giuridico per l'identificazione elettronica, il riconoscimento delle firme elettroniche e dei servizi fiduciari all'interno dell'UE. Perciò lo Stato membro che dovrà tendere all'obiettivo appena citato dovrà anche emanare delle sanzioni, chiarimenti nel rispetto dei principi emanati dal Reg. cit. In riferimento e per approfondire il tema dei principi e delle competenze dell'Unione Europea: BORGATO, CARDIN, DONA', DELLA GIUSTA, TRABUCCO, *Lineamenti di diritto pubblico*, Milano, 2020, p.68 ss.
Inoltre, si ricorda che un fondamento del principio di leale collaborazione si trova anche nella Costituzione italiana, con particolare riguardo all'art. 121.

Nonostante il margine di discrezionalità lasciato agli Stati membri, si ricorda che le sanzioni per le violazioni del diritto comunitario devono essere irrogate in maniera uniforme a quelle previste per le violazioni del diritto interno ([111]).

È quindi opportuno passare all'analisi dell'art. 32- *bis* CAD, rubricato "*Sanzioni per i prestatori di servizi fiduciari qualificati, per i gestori di posta elettronica certificata, per i gestori dell'identità digitale e per i conservatori"*.

L'organismo che può irrogare le sanzioni per le violazioni degli obblighi sanciti dal regolamento eIDAS è l'AgID e le sanzioni variano a seconda dei soggetti che compiono la violazione.

Nel caso di inadempienze da parte di prestatori di servizi qualificati, gestori di posta elettronica certificata, gestori di identità digitale e altri soggetti pubblici o privati, cui è stata affidata l'attività di conservazione dei documenti informatici della pubblica amministrazione, la pena pecuniaria irrogata va da un ammontare minimo di 40.000,00€ fino ad un importo massimo di 400.000,00€, fermo restando il diritto al risarcimento del maggior danno ([112]).

Qualora invece si profili la responsabilità di una pubblica amministrazione per la conservazione dei documenti informatici all'interno della propria struttura e in violazione dei requisiti del Reg. cit., questa sarà chiamata a pagare tra i 4.000,00€ e i 40.000,00€.

Ulteriore spunto di riflessione in merito a questo tema è la sentenza della Corte di Giustizia dell'Unione Europea, n.423 del 2005 in materia di circolazione delle merci. Nel caso di specie oltre al principio della manca collaborazione tra due Stati membri, vi è anche quello per cui in mancanza di una normativa di armonizzazione sarà lo Stato membro a decidere come garantire i diritti presenti a livello europeo.

[111] Con la sentenza della Corte di Giustizia dell'Unione Europea, C-68/ 88 e con riferimento all'art.5 del Trattato sull'Unione Europea dove si disciplina che uno Stato membro debba imporre alle violazioni del diritto comunitario le stesse sanzioni applicate nel caso di violazione del diritto interno; il giudice ribadisce che: "*A tal fine, pur conservando la scelta delle sanzioni, essi devono segnatamente ve- gliare a che le violazioni del diritto comunitario siano sanzionate, sotto il profilo sostanziale e procedurale, in termini analoghi a quelli previsti per le violazioni del diritto interno simili per natura ed importanza e che, in ogni caso, conferiscano alla sanzione stessa un carattere di effettività, di proporzionalità e di capacità dissuasiva*".

[112] Il risarcimento al maggior danno è disciplinato dal diritto interno e in particolare è previsto dall'art. 1224 co.2. del c.c. Questo tipo di risarcimento ha natura risarcitoria e consiste nell'ulteriore danno provocato con il verificarsi della violazione di una norma giuridica nei confronti degli utenti finali. Nel caso di una obbligazione pecuniario è l'ulteriore danno patito dal creditore pecuniario e non coperto con il pagamento degli interessi di mora da parte del debitore. Affinché avvenga questo ulteriore risarcimento dovrà essere accertata la colpevolezza dell'inadempimento dell'obbligazione e dovrà essere provato il nesso di causalità tra la condotta del debitore e il danno patrimoniale lamentato dal creditore. Rif: CENDON, *Responsabilità civile- volume terzo,* Milano, 2020, p.4535 ss.

Inoltre, nei casi di particolari gravità, l'Agenzia potrà disporre la cancellazione del responsabile dall'elenco dei soggetti qualificati.

Si ricorda però che l'AgID non potrà procedere direttamente con l'imposizione di una sanzione pecuniaria, in quanto c'è un criterio di gradualità da rispettare. Prima dovrà infatti richiedere ai soggetti che sono incorsi in irregolarità o inadempimenti di conformarsi, entro un termine fissato, agli obblighi previsti sia dalla normativa comunitaria che da quella nazionale. Solo se tale richiesta rimarrà disattesa, l'Agenzia potrà procedere con l'irrogazione della pena pecuniaria.

2.5 VALIDITÀ DELL' ATTO

La funzione principale della validazione temporale è quella di garantire l'esistenza del documento informatico in un determinato momento.

Con riguardo agli istituti tradizionali del diritto non è una novità la necessità di individuare con adeguata certezza il momento di formazione del documento analogico. L'atto pubblico o la scrittura privata autenticata sono riconosciuti come validi anche nei confronti dei terzi in quanto redatti o autenticati da notaio.

Quanto alla scrittura privata non autenticata la situazione è più complessa: "*La data della scrittura privata della quale non è autenticata la sottoscrizione non è certa e computabile riguardo ai terzi, se non dal giorno in cui la scrittura è stata registrata o dal giorno della morte o della sopravvenuta impossibilità fisica di colui o di uno di coloro che l'hanno sottoscritta o dal giorno in cui il contenuto della scrittura è riprodotto in atti pubblici o, infine, dal giorno in cui si verifica un altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento.*
La data della scrittura privata che contiene dichiarazioni unilaterali non destinate a persona determinata può essere accertata con qualsiasi mezzo di prova.
Per l'accertamento della data nelle quietanze il giudice, tenuto conto delle circostanze, può ammettere qualsiasi mezzo di prova" ([113]).

[113] Anzitutto preme ricordare che la data nella scrittura privata non è elemento essenziale se non in certi casi previsti dalla legge come nel caso del testamento olografo. Tuttavia, la data di una scrittura privata non autenticata rileva nei confronti dei terzi quando questa è stata riconosciuta (tacitamente o espressamente) dalla parte contro la quale è stata prodotta. Rif. CIAN, TRABUCCHI, *Commentario al Codice civile*, cit., sub art. 2704, pag. 3594.

Come emerge dal disposto letterale della norma, l'elencazione delle modalità con cui si può attribuire data certa ai sensi dell'art. 2704 c.c. non è tassativa ma si tratta piuttosto di una categoria aperta ([114]).

Passando ora alla validazione temporale elettronica ci si è chiesto se questo processo è in grado di assicurare data e ora certi sia valido anche nei confronti dei terzi.

Ancora una volta il rimando è all'art. 2704 c.c. e in particolare alla parte finale dove si prevede che *"La data della scrittura privata della quale non è autenticata la sottoscrizione non è certa e computabile riguardo ai terzi, [...] dal giorno in cui si verifica un altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento".*

Il quesito che si è posto è se questa norma possa essere suscettibile di un'interpretazione evolutiva e se, nello specifico, possa trovare applicazione al processo di validazione temporale elettronica. La dottrina si suddivideva principalmente in due fazioni tra quelli che consideravano il dettato della norma rigido e tra coloro che invece credevano ad una possibile lettura evoluzionistica. Chiaramente si è deciso di optare per una lettura evoluzionistica della norma, facendoci rientrare così anche la validazione temporale elettronica ([115]).

---

[114] I casi previsti dall'art. 2704 c.c. secondo i quali la data è certa e computabile anche nei confronti dei terzi sono diversi tra i quali si ricordano: il giorno in cui la scrittura è stata registrata e il giorno della morte o della sopravvenuta impossibilità fisica dei soggetti che l'hanno sottoscritta.
Tuttavia, come si è già anticipato, esistono altri casi non espressamente citati nella disposizione nei quali la data è certa e computabile anche verso i terzi. In generale, ci si riferisce ai casi che sono stati oggetto di una valutazione da parte del giudice di merito e per il quale il giudice ha deciso in modo positivo. Rif. CIAN, TRABUCCHI, *Commentario al Codice civile*, cit., sub. art. 2704, pag. 3594.

[115] Cfr. DELFINI e FINOCCHIARO, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, cit., p. 316, dove si spiega che la dottrina si era dimostrata contraria all'estensione della lettura dell'art. 2704 c.c. per i documenti informatici perché la normativa speciale non conteneva alcun riferimento espresso all'art. *de qua*. Si è però evidenziato come questa argomentazione non sia convincente dal momento che la disciplina dettata dal codice civile è di portata generale e perciò non necessita di richiami diretti per poter essere applicata. È evidente, perciò, che si debba procedere secondo una interpretazione evolutiva delle categorie civilistiche verso quelle che governano il contesto digitale.
Detto ciò, è importante rilevare che anche il Regolamento eIDAS mette in luce questo aspetto di progresso comparando la sottoscrizione autografa alla firma elettronica qualificata (ex. art. 25 par. 2).
Infine, va ricordato che mediante il d.l. n. 185 del 2008 è stato introdotto nel codice civile l'art. 2215-*bis* rubricato "*Documentazione informatica*". L'articolo in esame prevede che la marca temporale rilevi anche per la tenuta delle scritture contabili e dei libri sociali in forma elettronica. Rif: NAVONE, *Instrumentum digitale. Teoria e disciplina del documento informatico*, cit., p.201.

Tuttavia, è cruciale quanto previsto all'art. 20, co.1-*bis* CAD, dove si esplicita che: *"[...] La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida"*.

In base a quanto appena introdotto si passerà ora all'analisi della normativa comunitaria prima e solo in un secondo momento alla normativa nazionale.

Il regolamento eIDAS disciplina all'art. 41 gli "*Effetti giuridici della validazione temporale elettronica"* ([116]).

È dal dettato di questa norma che si comprendono gli effetti giuridici della validazione temporale elettronica qualificata o non qualificata.

La validazione temporale elettronica qualificata è disciplinata al co. 2 e gode della presunzione di accuratezza delle date e dell'ora e dell'integrità dei dati ad esse associati. Questo regime di presunzione deriva dal fatto che affinché una validazione temporale elettronica possa essere considerata tale deve rispettare cumulativamente i requisiti dell'art. 42 dello stesso regolamento. Vale a dire che il regime in esame deriva esattamente dal fatto che vi sono delle garanzie ricollegate alla stessa qualifica della validazione, tra le quali: la fonte di misurazione deve essere accurata, si deve escludere qualsiasi modifica non rilevabile dei dati e ancora il tutto deve avvenire grazie all'intermediazione di trust service provider.

Inoltre, questa tipologia di validazione, in base al par. 3 dell'art. 41, gode del principio del mutuo riconoscimento da parte dei singoli Stati membri. Il tema dell'equivalenza giuridica e dell'interoperabilità giuridica e tecnica degli e-trust services vede il suo fondamento nel caso della sola validazione temporale elettronica qualificata; data la presunzione di accuratezza appena citata, un altro Paese membro dell'Unione, non potrà che riconoscere come valido il time stamping, e quindi in grado di produrre gli effetti giuridici previsti dall'art. 41.

---

[116] *"1. Alla validazione temporanea elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporanea elettronica qualificata.*
2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.
3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri".

L'unico paragrafo dedicato alla validazione temporale non qualificata è il primo. La validazione temporale elettronica *de qua* manca in tutto o in parte dei requisiti sanciti dall'art. 42 del cit. Reg. e per questo motivo non può godere del regime di presunzione di accuratezza della data e dell'ora e di integrità dei dati utilizzati. Nonostante ciò, vige qui il principio della irrilevanza della materia per il quale non possono comunque essere negati effetti giuridici alla validazione temporale semplice per il solo motivo di realizzarsi in formato elettronico. Dato il progresso tecnologico e il possibile impiego di diversi strumenti elettronici di datazione, la valenza probatoria di questa tipologia di datazione è rimessa al libero apprezzamento del giudice ([117]).

Quanto alla disciplina nazionale la normativa in merito alla validazione temporale elettronica non quella esclusivamente disciplinata dal Codice dell'Amministrazione Digitale ma è necessario un coordinamento con i diversi d.p.c.m.

Ciò che è utile al fine della presente analisi è l'art. 20 co.1-*bis* ultimo periodo del cad dove si disciplina che "*La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida*" e ancora il co.3 del medesimo articolo "*Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica, sono stabilite con le Linee guida*".

In base a quanto spiegato sin qui, si è compreso che il CAD e, in particolare, l'art. 20 necessita di una lettura combinata con gli articoli d.p.c.m. del 2 febbraio 2013. Dalla lettura di tutto ciò si è in grado di comprendere il valore legale della validazione temporale elettronica dove data e ora saranno opponibili nei confronti dei terzi quando apposte in conformità alle regole tecniche ([118]).

---

[117] Il discorso appena accennato si ritrova, *mutatis mutandis*, anche alla situazione venutasi a creare con la firma elettronica semplice, la cui valenza probatoria viene lasciata al prudente apprezzamento del giudice, che determinerà la valenza probatoria della firma semplice, anche, in base alle caratteristiche informatiche dello strumento di firma utilizzato. In poche parole, qualora non ci fossero garanzie predeterminate circa l'utilizzo di determinate tecnologie, come nel caso in cui la validazione temporale venga certificata da un prestatore di servizi fiduciari qualificati che per essere considerato tale deve di per sé rispettare i requisiti del Regolamento, spetterà al giudice compiere una valutazione caso per caso in base alle tecniche utilizzate.

[118] Le regole tecniche *de qua* sono quelle enunciate nell'Titolo IV del d.p.c.m. del 2 febbraio 2013, con particolare riferimento agli articoli dal 47 al 52 e rubricato "*Regole per la validazione temporale mediante marca temporale".*

Di rileva fondamentale è l'art. 41 co. 1 e 2 del d.p.c.m. dove si prevede che *"1. I riferimenti temporali realizzati dai certificatori accreditati in conformità con quanto disposto dal titolo IV sono opponibili ai terzi ai sensi dell'art. 20, comma 3, del Codice.*

Infine, preme ricordare che anche nel caso della validazione temporale, come per la firma elettronica, si parla di un certificato digitale suscettibile di scadenza. In particolare, l'art. 53 d.p.c.m. 2013 prevede che: "*1. Tutte le marche temporali emesse da un sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a venti anni ovvero, su richiesta dell'interessato, per un periodo maggiore, alle condizioni previste dal certificatore.*
2. La marca temporale è valida per il periodo di conservazione, stabilito o concordato con il certificatore, di cui al comma 1".

Si può concludere che la validazione temporale elettronica e gli altri riferimenti temporali apposti secondo quanto dettato dall'art. 41 d.p.c.m. 2013 sono idonei a garantire data e ora certi ad un documento informatico ([119]).

2. I riferimenti temporali apposti sul giornale di con- trollo da un certificatore accreditato, secondo quanto indicato nel proprio manuale operativo, sono opponibili ai terzi ai sensi dell'art. 20, comma 3, del Codice".

[119] A ribadire quanto fin qui analizzato è una recente Sentenza della Cass. Civ., sez. I, n. 12939 del 23/05/2017, , prevede che: "*In presenza di documento informatico munito di marca temporale, è onere della parte interessata a negare la certezza della data, allegare e provare la violazione delle regole tecniche sulla validazione temporale, al rispetto delle quali l'art. 20, comma 3, CAD subordina l'opponibilità ai terzi della data (e dell'ora) apposta al documento informatico da certificatore accreditato e iscritto nell'elenco di cui all'art. 29, comma 6, CAD (nel testo anteriore alle modifiche introdotte dal d. lgs. n. 179/2016)".* In riferimento all'appena citata sentenza si sofferma anche VITRANI, *Gli effetti della marcatura temporale nel processo civile*, Giurisprudenza commentata del 27 giugno 2017, in *IUS Processo Telematico*, nel quale commento si chiede se un documento munito di marca temporale, apposto da un certificatore accreditato, è, ai sensi dell'art. 29 CAD, effettivamente munito di data certa. Sono due gli orientamenti che si individuano sul tema della validità della marcatura analogica del documento nei confronti dei terzi. Da un lato chi sostiene che il servizio reso da Poste Italiane nell'atto di validità della marcatura sia valido anche nei confronti dei terzi, in quanto apposto da un soggetto pubblico (Cass. Civ. sez. I con sentenza n.8438 del 28/05/2012). Diverso è invece il pensiero nei confronti di un servizio reso da un soggetto privato, il quale non avendo alcun poter di autorità pubblica, non potrà applicare una marca temporale valida (Cass. Civ. sez. I, sentenza n.26778 del 22/12/2016). In particolare, mediate una lettura coordinata con l'art. 29 CAD, si legge proprio che gli erogatori di tali servizi sono posti tutti in condizioni di parità e che pertanto, al termine dell'attività di certificazione anche una marca temporale apposta da un soggetto privato, nel rispetto delle regole tecniche, è valida.
E la Giustizia amministrativa con Consiglio di Stato, sez. III, n.4050 del 03/10/2016, in *DeJure.it,* in materia di inviolabilità delle offerte nelle gara telematiche è garantita dall'apposizione della firma elettronica e della marca temporale, prevede che: "*Nelle gare telematiche, con l'apposizione della firma e marcatura temporale, da effettuare inderogabilmente prima del termine perentorio fissato per la partecipazione, e con la trasmissione delle offerte esclusivamente durante la successiva fase di finestra temporale, si garantisce la corretta partecipazione e inviolabilità delle offerte; i sistemi provvedono, infatti, alla verifica della validità dei certificati e della data e ora di marcatura; inoltre l'affidabilità degli algoritmi di firma digitale e marca temporale garantiscono la sicurezza della fase di invio/ricezione delle offerte in busta chiusa*".

CAPITOLO 3: MARCA TEMPORALE TRA FUNZIONE E ASPETTI TECNICI

Sulla scorta di quanto fin qui analizzato si ritiene utile delineare in maniera quanto più completa possibile gli aspetti e le procedure che caratterizzano l'applicazione di una marca temporale ad un documento informatico.

Innanzitutto, preme sottolineare che, le regole tecniche contenute nel d.p.c.m. del 22 febbraio 2013 ([120]), i vari documenti riguardanti pareri tecnici e, ancora, i diversi strumenti informatici che si analizzeranno, non rappresentano un punto di partenza né, tantomeno, un punto di arrivo per l'analisi di questa materia.

Invero, una rinomata previsione, conosciuta dai più come "Legge di Moore", prevede che la complessità di un processore raddoppi ogni 18 mesi ([121]).

Prima di passare all'analisi degli aspetti operativi del procedimento di marcatura temporale, preme identificare la parte fidata che generalmente svolge l'attività di marcatura temporale. Si tratta di una *time stamping authority (tsa)* ossia di un prestatore di servizi fiduciari la cui funzione è quella di svolgere l'attività di certificazione temporale di un documento informatico ([122]).

---

[120] D.p.c.m. del 22 febbraio 2013 in materia di "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 2, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*" modifica il precedente d.p.c.m. del 30 marzo 2009 in considerazione delle modifiche apportate dal nuovo Codice dell'Amministrazione Digitale.

[121] Gordon Earle Moore, importante imprenditore e informatico statunitense che ha ricoperto un ruolo importante nella storia del Novecento sino alla sua morte nel marzo 2023, è noto ai tanti per l'elaborazione della Legge di Moore. È evidente che l'utilizzo del termine "legge" sia improprio, infatti non ha nulla a che vedere con una legge scientifica ma si tratta piuttosto, di una previsione informatica. La previsione venne elaborata nel 1965 e mediante questa, Moore, sosteneva che il numero dei transistor (dispositivi elettronici in grado di controllare il passaggio della corrente in un circuito elettronico) in ogni computer fosse destinato a raddoppiare periodicamente. Inizialmente, ogni 12 mesi ma dopo una serie di analisi si è giunti alla conclusione che dovrebbe raddoppiare ogni 18 mesi. Ciò che si rivela importante in questa previsione è che i dispositivi, che compongono un computer, sono in costante potenziamento soprattutto in termini di velocità e molteplicità delle operazioni che possono essere eseguite. Per tutto ciò è chiaro che si tratti di un settore in costante sviluppo. Rif. VITERBO, CODIGNOLA, *Le macchine di Touring, la legge di Moore e l'uomo bioinformatico*, in *Dir. Informatica*, fasc.3, 2008, p.321.

[122] I requisiti che un *TSA* deve soddisfare sono proposti nell'RFC 3161.
L'RFC, abbreviazione di Requests for Comments, è un documento pubblicato dall'RFC Editor e recante nuove innovazioni, specifiche tecniche o proposte delle comunità internazionali per definire standard di gestione e sviluppo delle reti e di internet.
L'RFC di riferimento per il servizio fiduciario di *TSA* è il numero 3161 nella sua versione di agosto 2001. Al paragrafo 2 vengono elencate le caratteristiche che un *TSA* deve avere. Tra le quali deve essere utilizzato una fonte e un valore di tempo affidabili; deve essere incluso un integrer (intero nel senso della tipologia di dato) che deve essere stato generato unicamente per un unico time-stamp token e, inoltre, deve essere incluso un identificatore univoco per ogni time-stamp. Infine, viene ribadito la funzione principiale del

Va da sé, che questo tipo di attività, solo se svolta nel rispetto delle regole vigenti, sarà in grado di assicurare data certa e opponibile ai terzi ad un documento informatico; in altre parole, sarà idonea a dimostrare che un dato documento esisteva prima di un determinato momento.

3.1 FUNZIONE DELLA MARCA TEMPORALE

Se la funzione della firma elettronica è quella di garantire la corretta identificazione del firmatario, affinché il messaggio da lui sottoscritto non sia ripudiabile in futuro ([123]); la funzione della marca temporale sarà quella di garantire l'istante in cui l'azione o un messaggio vengono generati.

Qualora gli algoritmi ([124]) di firma o di autenticazione fossero compromessi o per bravura dell'*eavesdropper* (dell'intercettatore, si può dire in italiano) o più semplicemente perché l'intero sistema di autenticazione è compromesso, come nel caso di perdita di segretezza verrebbero meno anche le garanzie di sicurezza.

Ad esempio, la perdita di divulgazione delle informazioni potrebbe causare la scoperta, da parte di un soggetto non autorizzato del codice di sicurezza (codice *pin)* di un bancomat e perciò il sistema di autenticazione sarà forzato.

TSA: contrassegnare solo con data e ora la rappresentazione hash del dato, ossia utilizzare un'impronta associata ad una funzione di hash.

[123] Si ricorda che la funzione principale della firma digitale (*digital signature*) è quella di assicurare un'associazione corretta tra l'identità del soggetto firmatario e le informazioni da lui sottoscritte. La firma digitale viene utilizzata in diversi ambiti della vita quotidiana, ad esempio per cifrare il testo di una e-mail ovvero per garantire la sicurezza nelle transazioni economiche. Il processo di corretta identificazione del firmatario prevede l'utilizzo della chiave privata del mittente per cifrare il testo mentre colui che riceverà il documento dovrà decifrare il testo mediante l'utilizzo della chiave pubblica. Questa tecnica garantisce l'integrità del messaggio e l'autenticità della sottoscrizione stessa da parte del firmatario. Tuttavia, si ricorda che il certificato di firma digitale ha durata limitata e per questo motivo si riconosce la necessità di apporre la marca temporale. Rif. Rif. DE ROSA, *Sistemi di cifratura*, Milano, 2004, p. 244.

[124] Per comprendere meglio: l'algoritmo racchiude tutte quelle istruzioni necessarie a raggiungere un preciso risultato data una determinata richiesta.
In CIACCI, BUONOMO, *Profili di informatica giuridica*, Milano, 2018, p.68 ss, il concetto di algoritmo è definito come quella "*procedura utile a risolvere un problema in un numero finito di passaggi".* Sarà il programmatore che si occuperà di scrivere un algoritmo prima in linguaggio di programmazione, ossia leggibile agli esseri umani, per poi tradurlo in linguaggio macchina per poter essere eseguito da un computer. Il concetto di algoritmo deriva da una nozione matematica e deriva dal grande matematico persiano Muhammad al-Khwarizmi vissuto introno all'800 d.C. Da qui il fatto che l'algoritmo matematico è il risultato di un numero finito di passaggi il cui fine è quello di risolvere un problema. Tuttavia, se l'algoritmo è inizialmente impregnato di riferimenti matematici in quanto utilizzato in questo ambito; ad oggi il suo utilizzo non appartiene esclusivamente a questo settore. Infatti, oggigiorno l'utilizzo di algoritmi attiene alla vita di tutti i giorni, anche se non sempre siamo consapevoli di utilizzare algoritmi. Se l'algoritmo è quel numero finito di passaggi necessari al raggiungimento di uno scopo allora anche quando seguiamo le istruzioni di montaggio di un mobile stiamo seguendo un algoritmo seppur in maniera inconsapevole; o ancora, quando compiamo tutte quelle azioni necessarie per fare un tè.

In altre parole, ciò che accade dopo la compromissione dei sistemi di autenticazione sfugge al controllo del soggetto autorizzato e comporta che l'*eavesdropper* possa falsificare o creare altri messaggi con la firma autenticata del soggetto derubato.

Per evitare tutto ciò, e perciò per garantire che la firma elettronica sia stata applicata in un momento anteriore alla perdita di segretezza, è necessario applicare la già nota marca temporale.

Lo scopo dell'apposizione di una marca temporale è di dimostrare il momento in cui il documento è stato generato. In questo modo, anche se in seguito ci fosse una compromissione dei sistemi di sicurezza, si sarebbe in grado di stabilire se la generazione della firma avvenne prima della compromissione.

Per fare tutto ciò ci si è avvalsi di strumenti informatici in grado di garantire, non solo l'autenticazione del soggetto e, perciò, la confidenzialità nelle conversazioni. La confidenzialità corrisponde alla capacità di escludere che persone sprovviste di specifica autorizzazione si avvalgano dell'informazione scambiata. (v. par. aspetti tecnici).

3.1.1 FASI DELLA VALIDAZIONE TEMPORALE ELETTRONICA

Per quanto riguarda l'aspetto operativo del procedimento di marcatura temporale, questo si può riassumere nei seguenti passaggi ([125]).

L'utente che vorrà usufruire del servizio in esame dovrà inoltrare al certificatore una "richiesta di validazione temporale". La richiesta, che avviene mediante il software fornito dal certificatore, deve contenere il *file* da marcare temporalmente oppure, in alternativa, l'impronta del *file* calcolata mediante la funzione di *hash*.

Inoltre, in base al software fornito, l'utente potrà anche selezionare il formato di marca temporale tra quelli disponibili ([126]). A titolo di completezza si accenna al fatto che il software di generazione di marca temporale potrà, anche, essere usato per compiere

[125] Rif. NAVONE, *Instrumentum digitale. Teoria e disciplina del documento informatico,* cit., p.197.

[126] Attualmente si individuano quattro diversi formati per la marca temporale. Il formato TSR (*time stamp response*) è il formato più semplice e contiene non tutto il file bensì solo l'impronta del file e l'evidenza informatica della marcatura. Il formato M7M contiene quanto spiegato per il formato TSR ossia l'evidenza della marca temporale e, inoltre, il file stesso sottoposto a marcatura. Il formato TSD (*time stamped data)* è il formato standard che contiene la marca temporale associata al documento stesso. Infine, il formato PDF è quello più utilizzato e prevede la possibilità di incorporare in sé sia la firma digitale che la marca temporale. Rif. GIACALONE, *Il ciclo di vita di un documento informatico: gestione e aspetti normativi*, cit., p. 84.

attività di verifica per appurare che la marca sia stata creata correttamente e che il certificato sia ancora valido.

Dopo la ricezione di tutti questi documenti, il prestatore (di servizi fiduciari) applicherà la marca temporale.

Le informazioni contenute nella marca temporale, oltre a quelle di data e ora, devono essere idonee a verificare l'autenticità della marca medesima ([127]).

Prima di rinviare al cliente il documento validato, il certificatore dovrà occuparsi di firmare digitalmente il file.

Sarà poi il richiedente, che dal momento della ricezione di quanto richiesto, dovrà occuparsi di conservare il documento cui viene apposta la marca temporale e la firma digitale.

Nel titolo IV del d.p.c.m. del 22 febbraio 2013, rubricato "*Regole per la validazione temporale mediante marca temporale"* e in particolare all'art. 54 sono indicate le operazioni necessarie per la richiesta della marca temporale ([128]).

Vengono, innanzitutto, spiegate le modalità per la richiesta di validazione temporale elettronica: queste sono decise dal certificatore e sono consultabili dall'utente, che vuole usufruire del servizio, nel manuale operativo ([129]).

---

[127] Le informazioni che devono essere contenute nella marca temporale sono elencate all'art. 48 del d.p.c.m. del 22 febbraio 2013, e ancora prima erano contenute nel d.p.c.m. del 30 marzo 2009.
Una marca temporale, in base a quanto previsto dal d.p.c.m., deve contenere almeno: "*a) identificativo dell'emittente; b) numero di serie della marca temporale; c) algoritmo di sottoscrizione della marca temporale; d) certificato relativo alla chiave utilizzata per la verifica della marca temporale; e) riferimento temporale della generazione della marca temporale; f) identificativo della funzione di hash utilizzata per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale; g) valore dell'impronta dell'evidenza informatica*". Inoltre, in base all'ultimo requisito la marca temporale può contenere anche un Codice identificativo dell'oggetto a cui appartiene l'impronta dell'evidenza informatica.

[128] Ex. Art. 54: *"1. Il certificatore stabilisce, pubblicandole nel manuale operativo, le procedure per l'invio della richiesta di marca temporale.*
2. La richiesta contiene l'evidenza informatica alla quale applicare la marca temporale.
3. L'evidenza informatica può essere sostituita da una o più impronte, calcolate con funzioni di hash scelte dal certificatore tra quelle stabilite ai sensi dell'art. 4, comma 2.
4. La generazione delle marche temporali garantisce un tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, non superiore al minuto primo".

[129] Il manuale operativo è un documento pubblico che definisce l'insieme delle procedure applicate dall'Ente Certificatore per svolgere la propria attività, nel caso in esame le informazioni inerenti alla procedura di validazione temporale.
È interessante per comprendere meglio in cosa consiste un manuale operativo quello pubblico da InfoCert S.p.A. quale servizio fiduciario qualificato e correttamente iscritto negli elenchi di fiducia pubblicai da

Invece, con riguardo alla richiesta da parte del soggetto che vuole che il suo documento venga validato, questa deve contenere l'evidenza informatica stessa ovvero può essere sostituita da una o più impronte di hash dell'evidenza (v. par. la funzione di hash).

3.1.2 DATA E ORA NELLA MARCA TEMPORALE

Il sistema che si propone di marcare temporalmente un documento, dopo aver ricevuto l'impronta dello stesso ovvero il file medesimo, dovrà associare data e ora, ottenendo così la validazione temporale del documento.

Va da sé che la data e l'ora ricoprono un ruolo importante in quanto è chiara la necessità di garantire, con un elevato livello di certezza, l'esatto momento temporale di apposizione della marca temporale.

Data e ora dovranno, perciò, conformarsi a protocolli internet al fine di migliorare coerenza e interoperabilità tra Paesi così da creare una base affidabile affinché pubbliche amministrazioni e soggetti, pubblici e privati, condividano gli stessi riferimenti temporali.

Ancora il d.p.c.m. del 22 febbraio 2013 è importante in questa analisi in quanto disciplina l'aspetto della precisione del riferimento temporale.

L'articolo 41, co. 2 e 3 prevede che: "2. *I riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato, secondo quanto indicato nel proprio manuale operativo, sono opponibili ai terzi ai sensi dell'art. 20, comma 3, del Codice.*
3. L'ora assegnata ai riferimenti temporali di cui al comma 2 del presente articolo, deve corrispondere alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591, con una differenza non superiore ad un minuto primo".

E ancora, l'art. 51 rubricato "*Precisione dei sistemi di validazione temporale" stabilisce che: "1. Il riferimento temporale assegnato ad una marca temporale coincide con il*

AgID. Il documento identificato mediante codice ICERT-INDI-TSA e datato 13/05/2022 contiene tutte le informazioni inerenti alla prestazione del servizio qualificato e non qualificato di validazione temporale. Il manuale, tra le diverse cose, indica le fasi della richiesta della validazione temporale. Il richiedente dovrà procedere alla richiesta mediante l'utilizzo del software predisposto a tale scopo e fornito da InfoCert, la richiesta deve inoltre contenere l'impronta del documento che si vuole sottoporre a validazione. Ancora vengono analizzati gli elementi che caratterizzano l'emissione della marca temporale ossia la precisione di data e ora di generazione del time-stamp, la struttura dati deve contenere delle informazioni specifiche e il tutto deve essere sottoscritto digitalmente. Questi sono solo degli esempi rispetto alle informazioni contenute nel manuale.

momento della sua generazione, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591.
2. Il riferimento temporale contenuto nella marca temporale è specificato con riferimento al Tempo Universale Coordinato (UTC)".

Dagli articoli sopra riportati è chiara la necessità che l'ora associata al riferimento temporale corrisponda alla scala di tempo *UTC ([130])*.

Inoltre, sempre in riferimento alla disposizione legislativa si trova la dicitura *UTC(IEN)*. La denominazione *UTC* indica, come appena analizzato il fuso orario internazionale, mentre *IEN* è l'acronimo dall'Istituto Elettronico Nazionale e fino al 1° gennaio 2017 forniva il segnale orario ufficiale alla Rai ([131]).

I dati contenuti nel *timestamp* sono i riferimenti di data in inglese *date*, e tempo, in inglese *time*.

Per comprendere il formato della marca temporale si farà riferimento all'RFC 3339 del luglio 2002, catalogato "*Date and time on the internet: timestamp*". Si tratta di un documento tecnico che analizza il formato della validazione temporale elettronica ([132]).

---

[130] L'UTC, dall'inglese *Coordinated Universal Time,* è il fuso orario di partenza, dal quale si misurano poi, i fusi orario di ciascuno Stato. L'Italia utilizza il fuso orario dell'Europea Centrale, in inglese *Central European Time,* con acronimo *CET* e il fuso orario sarà perciò *UTC+1*, dove il *+1* indica l'ora di anticipo rispetto all'ora *UTC*. In caso di ora legale all'ora il fuso orario *UTC+2*.

[131] In riferimento l'allegato I del Decreto del Ministero dell'industria, dell'artigianato e del commercio datato 30 novembre 1993 n.591 dove sono previsti le unità di base del Sistema Internazionale di Misura, in particolare si riporta il punto 3 dove è disciplinata la grandezza "tempo":
Unita' di misura: secondo
Simbolo dell'unita': s
Il campione nazionale di tempo e' realizzato dall'Istituto Elettrotecnico Nazionale "G. Ferraris" (IEN) tramite un oscillatore agganciato in permanenza alla frequenza propria della transizione quantica dell'atomo di cesio stabilita dalla XIII Conferenza Generale dei Pesi e delle Misure (1967) con la definizione del secondo. Esso e' conservato mediante un orologio atomico a fascio di cesio, con incertezza relativa, stimata a livello di una volta lo scarto tipo, di +/- 3 x 10(elevato a - 13) per tempo di integrazione superiore a 10(elevato a - 5) s.
La scala di tempo nazionale e' generata dall'IEN dal campione
nazionale di tempo; essa prende il nome di UTC(IEN). La datazione di un evento sulla scala UTC(IEN) e' effettuabile con incertezza stimata a livello di una volta lo scarto tipo, di +/- 50 ns.
La differenza tra la scala UTC(IEN) e la scala internazionale UTC (Tempo Universale Coordinato), elaborata dall'Ufficio Internazionale dei Pesi e delle Misure, e' mantenuta entro il limite di +/- 2 (Micron s).
Ad oggi, è parte dell'istituto nazionale di ricerca metrologica (INRiM) e svolge, in Italia, la funzione di istituto metrologico nazionale.

[132] Già dall' introduzione dell'RFC 3339 vengono ribadite alcune fondamentali considerazioni come che la data e il tempo siano dell'epoca corrente e perciò tra il 0000AD e 9999AD. I timestamp sono espressi

Generalmente il formato più utilizzato è il seguente: *YYYY-MM-DD T HH:MM:SS Z*, dove:

- Y, corrisponde all'inglese *year*, ossia all'anno ([133]);
- M, in inglese *month*, è il mese ([134]);
- D dall'inglese *day*, il giorno;
- la lettera T serve a staccare l'indicazione di data e ora;
- H, *hour*, ossia l'ora;
- M, *minute*, i minuti;
- S, ad indicare in secondi (in inglese *second*);
- infine, la lettera Z sta ad indicare l'utilizzo del fuso orario UTC.

Un esempio di validazione temporale potrebbe essere: 1964-04-12T14:20:50.52Z. quanto appena scritto rappresenta il giorno 12 aprile del 1964, quanto all'ora, espressa in formato UTC indice le ore 14, minuti 20 e 50.52 secondi.

3.2 ASPETTI TECNICI

Fin qui si è sempre trattato di autenticità del documento informatico, integrità e certezza delle informazioni in esso contenute, e, ancora, identificazione e autenticazione sicura, ma senza mai, comprenderne dal punto di vista tecnico il significato.

Per tutti questi motivi e perciò per capire, finalmente, come tutte queste proprietà possano essere garantite, si esamineranno i principali strumenti informatici, ad oggi in uso, quali crittografia e funzione di hash.

secondo il fuso orario del tempo universale e sono in costante evoluzione in quanto si dovranno utilizzare le migliori pratiche in quel momento. Rif. 3339.

[133] In rif. RFC 3339, punto 3: "*Internet Protocols MUST generate four digit years in dates. The use of 2-digit years is deprecated. If a 2-digit year is received, it should be accepted ONLY if an incorrect interpretation will not cause a protocol or processing failure*". Da ciò deriva che la data dovrà necessariamente essere espresso in 4 digit (cifre). L'utilizzo di due cifre può avvenire solo qualora non provochi una interpretazione errata del protocollo oppure non provochi il fallimento del processo.

[134] Anche in merito ai numeri che devono identificare i mesi al punto 5.7 dell'RFC 3339 ci sono delle indicazioni. Semplicemente si tratta di una tabella in cui vi è una correlazione tra un numero e il mese, ad esempio 01 per indicare il mese di gennaio. È interessante il mese di febbraio perché sia che si tratta di un anno normale che di un anno bisestile, verrà identificato mediante il numero 02.

3.2.1 LA CRITTOGRAFIA

La crittografia è la tecnica che studia le modalità, di cui ci si può avvalere, per rendere indecifrabile un testo ai soggetti non autorizzati, rendendolo, così, noto ai solo destinatari legittimati ([135]).

Per comprendere ancora meglio il concetto di crittografia si vuole riportare qui l'etimologia del termine: crittografia deriva dal greco *kryptós*, nascosto e *graphía*, scrittura.

La crittografia non è utilizzata solo nell'ambito dell'*Information and Communication Technology (ICT),* in quanto si individuano i primi impieghi di questa tecnica sin dall'antichità ([136]).

Tuttavia, si ricorda che la crittografia, per come la intendiamo noi, ossia applicata alla sicurezza delle comunicazioni in rete, è stata applicata all'inizio principalmente in ambito militare e diplomatico ([137]).

---

[135] Prima di procedere con l'analisi preme fare una distinzione tra la crittografia e la steganografia.
Il termine steganografia deriva dal greco *steganós* ossia coperto e *gráphein*, scrivere, si tratta perciò della tecnica di occultamento di un messaggio. Ad esempio, Erodoto racconta che nell'antica Persia questa tecnica veniva utilizzata per nascondere i messaggi sulla testa degli schiavi. Per inviare un messaggio si rasava la testa dello schiavo, si aspettava che ricrescessero i capelli e solo dopo lo schiavo veniva inviato al destinatario, che avrebbe poi dovuto ri-rasare la testa per poter leggere il messaggio. Tuttavia, però si trattava di una tecnica utile per nascondere solo un messaggio: il messaggio in sé è nascosto ma il suo contenuto non è a sua volta "protetto". Diversamente, invece, la crittografia è una tecnica che non mira a nascondere un messaggio in sé ma piuttosto il suo contenuto. È evidente che il messaggio sia stato inviato ma è il suo contenuto che è stato criptato e perciò è leggibile solo per coloro che possiedono la chiave di lettura.

[136] La crittografia a chiave venne utilizzata fin dall'antichità e consiste nell'utilizzo di una chiave di codifica per scomporre un testo in una sequenza di caratteri non comprensibili alla collettività. Sarà solamente un destinatario autorizzato che sarà in grado di decodificare il messaggio servendosi di un cifrario.
La tecnica più utilizzata nell'antichità è nota come crittografia a trasposizione e consiste nel cambiare le posizioni delle unità di un testo in chiaro, secondo un determinato schema, così che il testo cifrato costituisca una permutazione del testo in chiaro. Tra coloro che utilizzarono questa tipologia di cifratura si ricordano i magistrati spartani, i c.d. efori, che utilizzarono la *scitala* per inviare messaggi ai militari all'estero. La *scitala* consisteva in un cilindro contente una striscia di cuoio dove il testo del messaggio veniva scritto in righe longitudinali. Chiaramente solo il destinatario era a conoscenza del cifrario utilizzato e della sua applicazione.
Anche Giulio Cesare utilizzò sistemi di crittografia, in particolare il sistema di trasposizione, per rendere incomprensibile il contenuto delle sue lettere private. Rif. CIACCI, BUONOMO, *Profili di informatica giuridica*, cit., p.230 ss.

[137] In campo militare echeggia la creazione della macchina ENIGMA ideata dal tedesco Arthur Scherbius nel 1918 e utilizzata, poi, dagli stessi tedeschi durante la Seconda Guerra Mondiale. Si tratta di una macchina a crittografia polialfabetica (questa tipologia di cifratura venne ideata da, colui che diventò, poi anche Presidente degli Stati Uniti d'America, ossia Thomas Jefferson). L'utilizzo di questo sistema permette che la cifratura di una stessa lettera possa cambiare in continuazione: questo deriva da un meccanismo per il quale la cifratura di ciascuna lettera in chiaro e cifrata cambia dopo la cifratura di ogni lettera. In questo modo il sistema è estremamente sicuro e affidabile, data la difficoltà di comprendere ogni singolo meccanismo di cifratura applicato. L'unico modo, grazie al quale gli avversari riuscirono a rendere

La crittografia qui analizzata è invece svincolata dall'ambito militare e diplomatico, e si applica, piuttosto, ad un ambito commerciale-privato, il che implica la necessità di individuare livelli di standardizzazione adeguati per permettere lo scambio di messaggi tra soggetti, enti o aziende diversi.

Fatte queste essenziali precisazioni si passa ora ad analizzare due tecniche convenzionali di cifratura ([138]):

- a chiave simmetrica,
- e, a chiave asimmetrica, anche nota come cifratura a chiave pubblica.

3.2.1.1 LA CRITTOGRAFIA SIMMETRICA

Questa tecnica di cifratura prevede l'utilizzo di una stessa chiave (di cifratura) sia per cifrare che per decifrare i messaggi: ciò significa che il mittente potrà cifrare un messaggio con la stessa chiave, che permetterà, poi, al destinatario di decodificare il messaggio.

---

le conversazioni, cifrate dei tedeschi, trasparenti fu mediante l'aiuto di Hans Thilo Schmidt che rese noti due manuali di istruzioni Enigma in cambio di un compenso (ad oggi l'equivalente di trentamila euro). Fu solo grazie a questo traditore e dopo moltissimi studi che i polacchi riuscirono a decriptare le conversazioni tedesche (il loro punto di forza oltre ad avere le foto dei manuali, fu che i tedeschi usavano la stessa chiave di cifratura per una giornata intera, di conseguenza tutte le conversazioni avvenute in uno stesso giorno venivano decriptate mediante la stessa logica). Tuttavia, i tedeschi si accorsero che vi erano delle terze parti non identificate che violavano la sicurezza dei loro messaggi, per questo motivo iniziarono a depistarli, riuscendo così a continuare ad utilizzare la macchina Engima ancora per diversi anni. Per concludere si può dire che il punto di svolta lo si deve allo studioso Alan Turing, che anche grazie alla collaborazione con un gruppo di crittoanalisti, riuscì a decriptare i messaggi Enigma. Questa scoperta è cruciale ed è anche grazie a questa che la durata della guerra si è abbreviata in modo significativo. Rif. DE ROSA, *Sistemi di cifratura*, cit., p. 5 ss.

[138] Si è utilizzato il termine "convenzionale" in quanto si tratta di tipologie di crittografia utilizzate da gran parte della società odierna.

In rif. ARTONI, mediante la pubblicazione del documento "*Applicazione, in campo militare, delle tecniche di crittografia quantistica associate alle comunicazioni satellitari per garantire comunicazioni strategico-operative sicure e capaci di adeguarsi efficacemente ad un moderno scenario net-centrico*" del 27 novembre 2019, in il Ce.Mi.S.S (Centro Militare di Studi Strategici), individua un'ulteriore tipologia di crittografia, oltre a quelle convenzionali (crittografia simmetrica e asimmetrica): quella quantistica. Si tratta di una tecnica di crittografia più sicura, che dovrebbe essere impiegata nelle organizzazioni governative, militari e finanziarie; soprattutto per assicurare elevati standard di segretezza alle conversazioni in quanto in grado di individuare eventuali intercettazioni da parte di terzi. Si basa su due archetipi da un lato l'impiego di fotoni di luce usati come sorgenti e dall'altro il principio di indeterminazione di Heisenberg. Secondo il principio di indeterminazione, il sistema quantistico è in grado di individuare l'intrusione su un canale e di provocare un disturbo che avvisa gli utenti legittimi dell'intrusione.

Quello che si vuole chiarire è che l'utilizzo del termine "convenzionale" dipende dal contesto in cui viene utilizzato.

Ad esempio, DE ROSA, in *Sistemi di cifratura,* cit., p. 205 utilizza il termine convenzionale per indicare le tecniche di crittografia di tipo simmetrico.

È chiaro, che l'utilizzo del termine convenzionale si riferisca sia alle tecniche di crittografia simmetriche che asimmetriche.

La certezza circa l'autenticità del messaggio, ossia che il contenuto del messaggio sia rimasto immutato, si ha solamente quando la chiave del destinatario è in grado di decifrare il messaggio inviato dal mittente.

Tuttavia, si tratta di una tipologia di cifratura circoscritta ai soli canali di comunicazione ad accesso limitato, in quanto lo scambio della chiave di cifratura deve avvenire in maniera sicura ([139]). L'esempio classico, dove questo sistema di cifratura è considerato sicuro, si ha quando la comunicazione della chiave privata avviene ad una riunione privata oppure quando colui che consegna la chiave ripone la massima fiducia nel soggetto che deve fare da tramite con l'altro destinatario.

Va da sé che nelle reti telematiche ad accesso pubblico questo tipo di cifratura non possa essere utilizzato, in quanto, data la moltitudine di soggetti, il grado di fiducia si abbassa drasticamente.

La compromissione, ossia la conoscenza della chiave crittografia da parte di un soggetto non autorizzato, comporta la perdita di sicurezza del successivo scambio di dati.

In questo contesto sono quattro le modalità di scambio proposte affinché non avvenga compromissione:

- generazione di una chiave e contestuale consegna fisica della stessa;
- ancora, generazione di una chiave, questa volta da parte di un'entità fidata, e conseguente consegna fisica;
- presenza di un precedente canale cifrato e utilizzo dello stesso cifrando la chiave nuova con la precedente;

[139] La necessità di garantire un adeguato livello di sicurezza nella condivisione della chiave tra mittente e destinatario rimane l'unico problema centrale di questa tipologia di cifratura. A titolo di conoscenza, i due principali protocolli informatici, HTTPS e SSL utilizzati affinché la trasmissione delle informazioni mediante internet avvenga in maniera sicura, si servono di un sistema di cifratura simmetrico. Inoltre, è interessante che l'utilizzo di una stessa chiave di cifratura (per cifrare e decifrare messaggi) in un computer sempre più moderno, coincida con un aspetto favorevole alla stessa cifratura, anche se intuitivamente può sembrare l'opposto. In poche parole, utilizzare computer sempre più efficienti in grado di operare con chiavi di grandi dimensioni è un aspetto di rilevante importanza se si considera che l'utilizzo di ciascun bit in più di lunghezza della chiave di cifratura raddoppia la difficoltà per l'intercettore. In altre parole, l'intercettatore dovrà fare molti più tentativi per scoprire la chiave di cifratura. L'unico aspetto al quale attualmente non si è in grado di trovare soluzione è l'avvenuta conoscenza, da parte di un terzo non autorizzato, della chiave di cifratura. Rif. BROOKSHEAR e BRYLOW, *Informatica, Una panoramica generale*, cit., p. 194.

- infine, esistenza di un server di chiavi che genera le chiavi che verranno usate per la comunicazione; ciascuna chiave verrà, poi, inviata mediante il canale cifrato posseduto da ciascuna entità.

Le prime due modalità di scambio appaiono fin da subito limitanti, poiché la consegna fisica presuppone un ambiente ristretto, come per esempio può essere quello militare o diplomatico.

La terza tecnica appare critica per il semplice fatto che, nel caso di intercettazione, la conversazione sarà trasparente, potendo le informazioni cifrate venire a conoscenza anche di soggetti non autorizzati.

L'ultima modalità proposta è quella preferibile in un'ottica di utilizzo di cifratura simmetrica; infatti, si utilizzerà un canale univocamente cifrato per trasmettere le chiavi di cifratura. Anche se per certi aspetti rimane una modalità limitante ([140]).

Tuttavia, i crittografi del Novecento sentono la necessità di studiare nuovi sistemi in grado di permettere trasmissioni crittografiche, anche senza che mittente e destinatario si comunichino la chiave.

Fu proprio nel 1974 che Whitfield Diffie e Martin Hellman, due crittografi statunitensi, riuscirono a trovare una soluzione al problema della sicurezza utilizzando calcoli logaritmici discreti in un campo finito ([141]). Questa tipologia di cifratura è usata ancora oggi: valutata come estremamente sicura, è nota come crittografia asimmetrica.

---

[140] La modalità di utilizzo di un canale univocamente cifrato prevede la creazione di un canale di cifratura di servizio nel quale verranno, poi, comunicate le chiavi di sessione. Il canale di servizio dovrà essere cifrato con delle chiavi master (*master key*) scambiate in modalità sicura e utilizzate per cifrare il canale di servizio che permetterà la comunicazione tra il server e ciascuna entità. Invece, le chiavi di sessione (*session key*) sono usate per le comunicazioni in cifra tra entità. Si tratta di chiavi temporanee che vengono create frequentemente. Quanto agli aspetti positivi sicuramente si individuano aspetti favorevoli per la facilità di gestione della rete e sicuramente il ridotto utilizzo di chiavi a lunga durata. Nonostante questo, però la criticità che permane riguarda lo scambio delle chiavi, questa volta non di sessione che tanto sono temporanee ma, quanto piuttosto, per le chiavi master. Queste ultime necessitano di essere comunicate in maniera sicura perché se queste vengono scoperte allora la certezza circa la comunicazione tra entità e server nello scambiare le schiavi di sessione viene meno. Rif. DE ROSA, *Sistemi di cifratura*, cit., p. 276.

[141] Il campo finito indica una struttura algebrica costituita da un numero finito di elementi. Il logaritmo di un numero corrisponde alla potenza alla quale un numero (base) deve essere elevato per ottenere quel numero. In termini matematici si scrive come segue: $x=log_a\, b \rightarrow b = a^x$.
In questo caso $log_a b$ corrisponde al logaritmo discreto di b in base a. Per calcolare il logaritmo discreto dato un campo finito $GF(_p)$ bisognerà definire la radice primitiva di un numero primo p e considerandolo come un numero le cui potenze generano tutti gli interi da *1* a *p-1*. Considerando la difficoltà cui ci si è imbattuti per spiegare quanto appena scritto e la necessità di impiegare numeri primi grandi per queste operazioni,

3.2.1.2 LA CRITTOGRAFIA ASIMMETRICA

La crittografia a chiave pubblica presuppone l'utilizzo di due chiavi di cifratura generate contemporaneamente e indissolubilmente legate da una relazione biunivoca ([142]).

In altre parole, vengono create e utilizzate due chiavi: una chiave verrà usata per la cifratura e l'altra per la decodifica del messaggio. L'utilizzo delle chiavi non è predeterminato, vale a dire che si può scegliere una chiave privata o pubblica per la cifratura, l'unico aspetto da tenere in considerazione è che una volta scelta la funzione della chiave, quella deve rimanere tale.

Ad esempio, la chiave privata può essere utilizzata per cifrare il testo in chiaro e la chiave pubblica per decifrare il messaggio, o viceversa. In questo modo la chiave pubblica sarà in possesso di tutti mentre quella privata sarà solamente del soggetto che ha originato il messaggio.

Sono quattro i principi che governano questa tipologia di cifratura:

- ogni utente possiede due chiavi;
- le chiavi sono unite tra loro da un rapporto di corrispondenza biunivoca: per una chiave K_1 esisterà solo una chiave K_2;
- la chiave di cifratura non può essere usata per decifrare e viceversa, comunque la scelta della chiave utilizzata per cifrare è indipendente;
- e, infine, la conoscenza di una chiave non permette di risalire all'altra grazie all'utilizzo di numeri primi molto grandi.

Ad oggi, per la cifratura asimmetrica si utilizza l'algoritmo RSA, ideato nel 1977, e la cui denominazione deriva dai cognomi dei suoi inventori R. Rivest, A. Shamir e L. Adleman ([143]). Si tratta dell'algoritmo che mette in pratica l'idea proposta da Diffie e Hellman.

Tuttavia, l'utilizzo della crittografia *de qua* presuppone la risoluzione di alcuni problemi legati all'utilizzo di una coppia di chiavi asimmetriche:

va da sé la difficoltà nel tentare di scoprire i numeri utilizzati per decifrare l'algoritmo. Rif. e per approfondire: DE ROSA, *Sistemi di cifratura*, cit., p. 213.

[142] Una relazione biunivoca è una relazione di equivalenza tale per cui in una relazione tra una chiave K_1 e un'altra chiave K_2, ad ogni chiave K_1 corrisponderà una e solamente una chiave K_2.

[143] Il documento di riferimento per questo algoritmo è l'RFC 8017 il cui scopo è quello di fornire raccomandazioni per l'implementazione della crittografia asimmetrica basata sull'algoritmo RSA.

- il problema del tempo che occorre per cifrare un documento, soprattutto se quest'ultimo contiene un testo molto lungo;
- la necessità di identificare il soggetto che rende nota la chiave pubblica cioè assicurare con un elevato livello di certezza che il soggetto che rende pubblica la chiave è quello che la possiede;
- infine, la possibilità da un elemento pubblico di ricavare la chiave privata è un problema che metterebbe in crisi l'affidabilità dell'intero sistema ([144]).

Il primo problema individuato, ossia il fatto che, codificare un testo lungo potrebbe richiedere maggior tempo per portare a termine l'operazione, è stato risolto predeterminando una lunghezza di caratteri fissi che possono essere utilizzati. La lunghezza della "stringa" ([145]) varia in base all'algoritmo utilizzato e tendenzialmente può variare dall'utilizzo di 160 bit oppure 128. Per eseguire questo tipo di operazione, il presupposto è lo sfruttamento della funzione di hash. (v. par. la funzione di hash).

Quanto al problema della necessità di assicurare l'identificazione inequivocabile del titolare della chiave pubblica, la situazione è risolta dalla figura dei certificatori, anche noti come prestatori di servizi fiduciari (v. par. 2.4).

Infine, l'ultima criticità individuata con riguardo alla crittografia asimmetrica è la possibilità di ricavare dalla chiave nota l'altra chiave. Questa possibilità è stata smentita fin dall'inizio e l'esempio è rappresentato dall'algoritmo RSA, per il quale risulta impossibile risalire alla chiave privata da quella pubblica. In poche parole, bisognerebbe conoscere il prodotto dei numeri primi utilizzati per generare una chiave, oltre a conoscere anche gli stessi numeri primi. E considerando che i numeri utilizzati sono molto grandi è impossibile individuarli.

Infine, come si è già analizzato per la crittografia simmetrica, anche per la crittografia asimmetrica il problema della vulnerabilità delle chiavi si verifica, sebbene, in maniera differente.

Se nella prima tipologia di cifratura il problema sussisteva quando la chiave doveva essere comunicata all'altro soggetto, nel caso *de qua* il problema sussiste quando lo scambio di

[144] Rif. CIACCI, BUONOMO, *Profili di informatica giuridica*, cit., p.229 ss.
[145] La stringa nel linguaggio informatico è una sequenza di caratteri, lettere, numeri o simboli; che viene utilizzata per rappresentare un testo.

messaggi avviene con soggetti che si fingono di essere la persona con cui si crede di dialogare oppure, nei casi più seri, con la perdita di efficacia del processo di firma digitale, in quanto, la firma usata per l'attività di verifica è associata alla chiave privata dell'ingannatore.

3.2.2 LA FUNZIONE DI HASH

Il termine *hash* deriva dall' omonima parola inglese "sminuzzare", si tratta perciò di una tecnica in grado di "tagliare", nel senso di trasformare, i dati informatici generando un output, nel senso di risultato, di lunghezza fissa.

La tecnica *de qua* è utilizzata principalmente per costruire sistemi di archiviazione efficienti e in particolare, costituisce uno dei sistemi all'origine della memorizzazione del recupero dei dati.

In questo caso il file hash è utilizzato per ricercare le informazioni, in particolare i dati contenuti all'interno di una memoria di massa ossia quella unità che si può aggiungere alla memoria principale per espandere la capacità di memorizzazione. Si tratta di un processo di recupero efficiente in quanto utilizzabile anche se il recupero riguarda record di file in un ordine non prevedibile ([146]).

Il processo di recupero consiste nell'applicare all'elemento da ricercare la funzione di hash alla sua chiave per determinare il *bucket* ([147]) appropriato. Quello che si otterrà sarà un file di hash. Qualora, invece, la ricerca fosse avvenuta in una memoria principale allora ciò che si andrà ad ottenere sarà una tabella di hash.

Questa tecnica non assolve però solo alla funzione di ricerca di dati ma può anche essere utilizzata come metodo di autenticazione per i messaggi trasferiti mediante internet. Vale a dire che, mediante l'utilizzo di una funzione segreta, il destinatario di un messaggio è in grado di verificare che il valore di hash da lui ottenuto sia lo stesso del messaggio originale: in questo modo ciò che si prova è l'integrità del messaggio.

---

[146] L'hashing è la tecnica che si favorisce rispetto a quella dell'indicizzazione poiché la prima tecnica non ha bisogno che il suo indice sia sottoposto a manutenzione diversamente, invece, da quanto richiesto per l'indicizzazione. Quest'ultima tecnica sfrutta un indice per individuare più rapidamente l'elemento che di vuole ricercare, l'indice contiene sia l'elenco delle chiavi che l'indicazione di dove è archiviato il record. Per tutto ciò se ne ricava che l'indice dovrà essere necessariamente aggiornato qualora ci fossero delle modifiche negli elementi contenuti. Rif. BROOKSHEAR e BRYLOW, *Informatica, Una panoramica generale*, cit., p. 421 ss.

[147] Il bucket, *strictu sensu* secchio, è la sezione di una memorizzazione di dati nella quali possono essere contenuti diversi record.

In questo caso un valore di hash, impronta del testo o *digest* è il risultato di un algoritmo non reversibile (chiaramente un algoritmo di hash) che, trasforma in maniera irreversibile un pacchetto di dati di qualsiasi lunghezza, in un output di lunghezza predefinito in base all'algoritmo utilizzato.

Dire che si tratta di un algoritmo irreversibile significa affermare che questo lavora in maniera unidirezionale: dall'output, ossia la stringa che si ottiene come risultato, non si è in grado di ricostruire il documento originale (*input*).

L'algoritmo di maggior utilizzo in questo ambito è denominato SHA, acronimo inglese di Secure Hash Algorithm.

La prima versione, SHA-1, è ormai considerata insicura dopo che è stato compromesso da crittoanalisti ([148]). Ad oggi la versione più nota è quella denominata SHA-256 (più comunemente SHA-2), dove il numero indicato nella sigla rappresenta la lunghezza del digest prodotto ossia di 256 bit ([149]).

3.3 LA SICUREZZA

Chiaramente l'utilizzo di nuove tecnologie informatiche presuppone anche la maggior diffusione di tecniche di sicurezza in grado di arrestare i fenomeni degli attacchi informatici, i c.d. *cybercrime*.

La necessità, per coloro che forniscono servizi fiduciari qualificati e non qualificati, di garantire adeguati livelli di sicurezza e integrità dei dati informatici è un presupposto fondamentale, per far sì che tutte quelle regole di diritto fin qui analizzate possano trovare applicazione.

Perciò un sistema per essere sicuro dovrà essere ben progettato e affidabile.

[148] SHA-1 è ormai obsoleta e non è più in grado di garantire elevati livelli di sicurezza è lo stesso *National Institute of Standard and Technology* (NIST) a dichiaralo non più sciuro e avvisando tutti coloro che ancora lo utilizzano a sostituirlo con le più recenti versioni, SHA-2 o SHA-3. Rif. *NIST retries SHA-1 Cryptographic Algorithm,* 15 December 2022, NIST. https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm

[149] Per approfondire il rimando è l'RFC 4634, del luglio 2006 e denominato *"US Secure Hash Algorithms (SHA and HMAC-SHA)".*

Generalmente è in riferimento ad un sistema operativo ossia un sistema che sovraintende le attività di un computer che si ravvede il compito essenziale di proteggere le risorse del computer.

Tuttavia, sono diversi i modi mediante i quali un soggetto non autorizzato può cercare di introdursi illegalmente in un computer.

L'attacco dall'esterno, prevede che l'*hacker* per mezzo di un *malware* (software dannoso) possa attaccare il sistema informatico. Tra i software dannosi più utilizzati si trovano: *virus* ossia software che infettano un computer inserendosi nei programmi già presenti e *worm* (dall'inglese verme), che sfruttando la rete, sono in grado di inserirsi autonomamente nel computer e di creare copie di sé stesso. Il cavallo di Troia, invece, è un programma, mascherato come un'applicazione utile, ad esempio un gioco, che viene installato dalla vittima inconsapevolmente. Ancora, esiste lo *spyware,* letteralmente programma spia, si tratta di un software in grado di tenere traccia di tutte le attività che l'utente copia all'interno del computer. Da ultimo, il *phishing*, è semplicemente un modo evidente per chiedere informazioni all'utente. Corrisponde in altre parole alla "pesca" di password.

Quanto all'attacco dall'interno, il maggior sistema utilizzato è conosciuto come DoS, dall'inglese *denial of service* e consiste nel sovraccarico di traffico Internet indesiderato e destinato ad un computer, in modo tale che il traffico normale non giunga alla destinazione prevista. Per questo tipo di attacco il computer, seppur inconsapevolmente, si presterà ad essere complice, per questo motivo è sempre importante installare aggiornamenti di sicurezza. Un altro esempio di attacco dall'interno è quello che deriva dagli *spam* o e-mail spazzatura, si tratta di messaggi indesiderati, che, comunque di rado sono in grado di sovraccaricare con successo il sistema ([150]).

Oltre al sistema operativo come metodo per proteggere quanto contenuto all'interno di un computer, anche l'utilizzo di una password correlata ad un account rappresenta il modo più conosciuto per controllare l'accesso alle informazioni.

Esiste, però, un'ulteriore tecnica in grado di assicurare adeguati livelli di sicurezza: la crittografia.

[150] Rif. BROOKSHEAR e BRYLOW, *Informatica, Una panoramica generale*, cit., p. 190 ss.

Anche se già analizzata, a titolo di completezza si ricorda che la crittografia è la tecnica che studia il modo di inviare e ricevere messaggi, sfruttando la cifratura, in modo tale che solo i soggetti autorizzati siano in grado di accedere alle informazioni.

In particolare, un crittosistema è tipicamente un insieme di algoritmi crittografici il cui fine è quello di fornire un particolare servizio di sicurezza. Solitamente si formano di tre algoritmi: l'algoritmo di crittografia, nel caso in esame quello RSA, l'algoritmo per la cifratura e, infine, uno per la decifratura.

Tuttavia, anche per questa tecnica si sono ipotizzati casi di violazione della sicurezza ([151]).

Questi metodi possono essere applicati sia all'algoritmo RSA che alla funzione di hash, anche se preme evidenziare che si tratta di tecniche che non necessariamente comportano un esito positivo ([152]).

Per quanto sin qui visto, la crittografia rimane ancora la tecnica più utilizzata e in grado di garantire un adeguato livello di sicurezza.

3.4 CASO PROCESSUALE

Qui di seguito, si analizzerà un caso processuale, al fine di rendere evidente l'importanza dell'apposizione di una marca temporale valida ed efficace, la quale può addirittura, ricoprire un ruolo cruciale nella risoluzione di una questione o nella decisione di una causa.

---

[151] Crittoanalisi è un termine di derivazione greca: discenda dalla combinazione di *kryptós*, nascosto e *analýein*, scomporre. Esso indica infatti l'insieme dello studio dei metodi per ottenere il significato di informazioni cifrate ma senza avere accesso alle informazioni segrete.

[152] Rispetto all'algoritmo RSA, utilizzato per la cifratura, si ipotizzano tre possibili modalità di attacco: la forza bruta (*Brute Force Attack)*, attacchi di natura matematica e attacco solo per conoscenza del testo cifrato. Il primo attacco avviene quando l'eavesdropper prova tutte le possibili combinazioni di chiave di cifratura, va da sé che questa tipologia di attacco si traduca in una modalità con improbabili tassi di successo data la dimensione utilizzata per la creazione delle chiavi. Negli attacchi di natura matematica si procede per fattorizzazione ossia mediante scomposizione del prodotto in fattori primi, anche in questo caso il successo è pari a zero in quanto allo stato attuale non esistono conoscenze matematiche adeguate e in grado di affrontare la fattorizzazione di due numeri primi. Quanto all'attacco mediante il quale presuppone di determinare la chiave privata considerando il tempo che l'algoritmo impiega per decifrare il messaggio. Ad ogni modo anche per ultima tipologia di attacco esistono metodi in grado di ovviare l'attacco.
Tuttavia, anche per la funzione di hash sono stati individuati degli attacchi che potrebbero comprometterne la sicurezza, si tratta, ancora una volta del *Brute Force Attack,* e la crittoanalisi della funzione di compromissione che si ha quando dato un hash se ne ricava il messaggio. Rif. DE ROSA, *Sistemi di cifratura*, cit., p. 378 ss.

La sentenza in esame è la n. 4251 della Cassazione civile, sez. I, datata 13/02/2019, in *DeJure.it* ([153]), nella quale si evidenzia il ruolo cruciale che l'apposizione della marca temporale ha avuto nella decisione della causa.

Il caso riguarda un giudizio di opposizione allo stato passivo, nel quale il Giudice di merito considerava non ammesso un credito relativo ad un rapporto di lavoro intercorso con l'azienda fallita; nel caso di specie, la marca temporale non era considerata valida. Il lavoratore decide, quindi, di fare ricorso dinnanzi alla Corte Suprema di Cassazione per violazione e falsa applicazione delle norme del Codice dell'Amministrazione Digitale.

Rispetto alla documentazione prodotta in giudizio si fa riferimento ad un CD contenente, in formato .pdf, diversi documenti informatici tra i quali: la lettera di assunzione, la lettera di dimissioni, il riepilogo delle ore di lavoro svolte dalla parte ricorrente e, il riconoscimento del debito da parte della società fallita. Con riguardo a quest'ultimo il documento era versato in atti *"[...] con relativa stampa di certificazione in formato cartaceo dal quale emergeva, innegabilmente, che allo stesso "era stata apposta la marca temporale in data 27 novembre 2012, alle ore 11:17:59" (e, quindi, in data ben anteriore a quella della dichiarazione di fallimento di (OMISSIS) s.r.l., intervenuta il 14 maggio 2013*)" ([154]).

Il Collegio prosegue analizzando il concetto di marcatura temporale considerandolo come il processo di generazione e apposizione di una marca temporale ad un documento elettronico ad opera di una terza parte fidata. Nel caso di specie, la parte fidata è Aruba Posta Elettronica Certificata s.p.a., Autorità di Certificazione dal dicembre 2017 e correttamente iscritta nell'Elenco Pubblico dei Certificatori accreditati.

Inoltre, considerata già la marca temporale valida e certa in quanto apposta in data 27 novembre 2012, alle ore 11.17:59 e perciò, certamente anteriore alla dichiarazione di fallimento (maggio 2012); il Collegio ribadisce che: "*la cd. "marca temporale" è un*

[153] Sul tema anche: NARDELLI, *La validazione temporale e l'efficacia probatoria nei confronti dei terzi,* in *ilprocessotelematico.it,* 2019, https://ilprocessotelematico.it/articoli/giurisprudenza-commentata/la-validazione-temporale-e-l-efficacia-probatoria-nei-confronti

[154] V. punto 3.1 della sent. cit., ove si legge anche che*"Se, dunque, - ha, poi, proseguito - "le copie di un documento (doc. nn. 3, 5, 6 e 7 fascicolo dott. B. opposizione stato passivo) verificate conformi agli originali da parte del Giudice Relatore all'udienza dell'8 aprile 2014... sono state munite di data certa il 27.11.2012 con marca temporale (che, tra l'altro, assicura che il documento dall'apposizione della marca temporale non possa essere più modificato), nessun dubbio può nutrirsi sull'anteriorità all'apertura del concorso (e quindi sull'opponibilità alla Curatela) dei documenti in questione"*. Rif: sentenza n. 4251, Cass. Civ., sez. I, datata 13/02/2019, in *DeJure.it.*

servizio specificamente volto ad associare data e ora certe e legalmente valide ad un documento informatico, consentendo, quindi, di attribuirgli una validazione temporale opponibile a terzi" ([155]).

Perciò:

- la marca temporale è da considerarsi valida ed efficace in quanto apposta anteriormente alla dichiarazione di fallimento della società fallita,
- l'apposizione della stessa è avvenuta mediante terza parte fidata,
- ed è riconosciuta dalla legge il cui fondamento normativo è il Codice dell'Amministrazione Digitale ([156]).

---

[155] Punto 3.3 *ibidem* chiarisce che: *"Rileva, inoltre, il Collegio che la cd. marcatura temporale è il processo di generazione ed apposizione di una marca temporale su un documento informatico, digitale o elettronico, consistente nella generazione, ad opera di una terza parte fidata (il Certificatore accreditato, nella vicenda oggi in esame si tratta di Aruba Posta Elettronica Certificata s.p.a., Gestore Certificato dal 12 ottobre 2006 ed Autorità di Certificazione dal 6 dicembre 2017, iscritta nell'Elenco Pubblico dei Certificatori accreditati da Digit PA), di una "firma digitale del documento" cui è associata l'informazione relativa ad una data e ad un'ora certa. L'apposizione della marca temporale consente, così, di stabilire l'esistenza di un documento informatico a partire da un certo istante e di garantirne la validità nel tempo"*.
Punto 3.3.1: *"In altri termini, la cd. "marca temporale" è un servizio specificamente volto ad associare data e ora certe e legalmente valide ad un documento informatico, consentendo, quindi, di attribuirgli una validazione temporale opponibile a terzi (cfr. D.Lgs. n. 82 del 2005, art. 20, comma 3, cd. Codice dell'Amministrazione Digitale). Il servizio di marcatura temporale, peraltro, può essere utilizzato anche su files non firmati digitalmente, parimenti garantendone una collocazione temporale certa e legalmente valida. La marca temporale, dunque, attesta il preciso momento in cui il documento è stato creato, trasmesso o archiviato. Infatti, quando l'utente, con il proprio software, avvia il processo di apposizione della marca temporale sul documento (informatico, digitale o elettronico), automaticamente viene inviata una richiesta contenente una serie di informazioni all'Ente Certificatore Accreditato (qui, come si è detto, individuato in Aruba), che verifica in maniera simultanea la correttezza della richiesta delle informazioni, genera la marca temporale e la restituisce all'utente. Questo processo automatico ed immediato garantisce la sicurezza e la validità del processo di marcatura"*. Rif: sentenza n. 4251 della Cassazione civile, sez. I, datata 13/02/2019, cit.

[156] Punto 3.4 della sentenza n. 4251 della Cassazione civile, sez. I, datata 13/02/2019, cit. : *"Il Codice dell'Amministrazione Digitale (D.Lgs. n. 82 del 2005), infine, definisce la validazione temporale come "il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi" (art. 1, comma 1, lett. bb), - lettera poi soppressa dal D.Lgs. 26 agosto 2016, n. 179, art. 1, comma 1, lett. h), a decorrere dal 14 settembre 2016, ai sensi di quanto disposto dall'art. 66, comma 1, del medesimo D.Lgs. n. 179 del 2016 - vigente ratione temporis), ed il suo successivo art. 20, comma 3, combinato con gli artt. 41 e da 47 a 54 del D.P.C.M. del 22 febbraio 2013 (recante Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli art. 20, comma 3, art. 24, comma 4, art. 28, comma 3, art. 32, comma 3, lett. b), art. 35, comma 2, art. 36, comma 2, e art. 71), chiariscono il valore legale della validazione suddetta sancendo, sostanzialmente, che la data e l'ora di formazione del documento informatico sono opponibili ai terzi ove apposte in conformità alle regole tecniche sulla validazione temporale. In particolare, l'art. 41 definisce i casi in cui riferimenti temporali sono opponibili a terzi, mentre gli artt. 47-54 definiscono le regole per la validazione temporale mediante marca temporale"*.

Per tutto ciò è evidente che la decisione del Tribunale di Bergamo nel dichiarare non valida la marcatura temporale è in violazione rispetto a quanto previsto dal Codice dell'Amministrazione Digitale, infatti, la Cassazione accoglie il ricorso.

Quindi, il ruolo della validazione temporale, nella decisione di questa causa, si è rivelato cruciale in quanto in grado di dimostrare l'effettivo credito del ricorrente nei confronti della società fallita.

CONCLUSIONE

L'apposizione di una marca temporale è quel processo in grado di indicare, con precisione, il momento di formazione, trasmissione o archiviazione di un documento elettronico. Tuttavia, si ricorda che sono in grado di assurgere a questa funzione anche altre tipologie di riferimento temporale, individuate, in concreto, all'art.41 del d.p.c.m. 22 febbraio 2013.

A livello europeo la validazione temporale elettronica può essere qualificata o non qualificata. Nel caso di una validazione temporale qualificata si può affermare che si tratta di un processo valido e in grado di produrre effetti giuridici quando rispettati i tre requisiti cumulativi individuati dal Regolamento eIDAS.

Con riguardo alla normativa italiana, il Codice dell'Amministrazione Digitale prevede che la marca temporale, derivante da una validazione elettronica qualificata renda il documento elettronico opponibile ai terzi quando apposta in conformità alle regole tecniche individuate da AgID.

Infine, si ricorda che tutto il procedimento di validazione temporale elettronica è rafforzato dall'utilizzo di strumenti informatici, quali crittografia e funzione di hash, che sono in grado di dimostrare se lo scambio delle informazioni è avvenuto in maniera tale da garantire l'integrità dei dati contenuti nei documenti o meno.

BIBLIOGRAFIA:

A. THIENE. *sub*. art. 2043, in *Commentario breve al Codice civile*, diretto da Cian e Trabucchi, Milano, 2022, p. 2236 ss;

Aa. Vv., *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*, a cura di Delfini e Finocchiaro, Torino, 2017;

ARTONI, *Applicazione, in campo militare, delle tecniche di crittografia quantistica associate alle comunicazioni satellitari per garantire comunicazioni strategico- operative sicure e capaci di adeguarsi efficacemente ad un moderno scenario net-centrico*, in *Ce.Mi.S.S, 27 novembre* 2019, < https://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/ricerche/Pagine/Artoni_Ita.aspx > (24/09/2023);

BORGATO, CARDIN, DONÀ, DELLA GIUSTA, TRABUCCO, *Lineamenti di diritto pubblico*, Milano, 2020;

BROOKSHEAR e BRYLOW, *Informatica, una panoramica generale*, Milano, 2020;

CARATTA, *Funzione dimostrativa della prova (verità del fatto nel processo e sistema probatorio)*, in *Rivista di diritto processuale*, 2001, p. 73;

CARNELUTTI, *La prova civile, parte generale, il concetto giuridico della prova*, Milano, 1992;

CASADEI e PIETROPAOLI, *Diritto e tecnologie informatiche*, Trento, 2021;

CAVALLONE, *Forme del procedimento e funzione della prova (ottant'anni dopo Chiovenda)*, in *Rivista di diritto processuale*, 2006, p. 417;

CEDON, *Responsabilità civile- volume terzo*, Milano, 2020;

CHECCHINI e AMADIO, *Lezioni di diritto privato*, Torino, 2020;

CHIOVENDA, *Principii di diritto processuale*, Napoli, 1980;

CIACCI e BUONOMO, *Profili di informatica giuridica*, Milano, 2018;

DE ROSA, *Sistemi di cifratura*, Milano, 2004;

DELFINI e FINOCCHIARO, *Diritto dell'informatica*, Milano, 2014;

DITTRICH, *Le prove nel processo civile e arbitrale*, Milano, 2021;

E. VULLO, *sub*. art. 2704, in *Commentario breve al Codice civile*, diretto da Cian e Trabucchi, Milano, 2022, p.3593 ss;

F. PORCU, *sub.* art. 130 c.p.p., in *Codice di procedura penale commentato- commento VI edizione-tomo I,* a cura di Giarda e Spangher, Milano, 2023, p. 1978 ss;

GENGHINI, *La forma notarile digitale*, Milano, 2022;

GIACALONE, *Il ciclo di vita di un documento informatico: gestione e aspetti normativi*, Milano, 2021;

HILBERT e LÓPEZ, *The World's Technological capacity to Store, Communicate and Compute Infromation,* in *Science*, 2011, p. 60;

IASELLI, *Diritto e nuove tecnologie*, Milano, 2016;

NARDELLI, *La validazione temporale e l'efficacia probatoria nei confronti dei terzi,* Giurisprudenza commentata del 04 aprile 2019, in *ilprocessoteematico.it*;

NAVONE, *Instrumentum Digitale. Teoria e disciplina del documento informatico*, Milano, 2012;

PATTI, *Commentario al codice civile*, *Libro sesto- della tutela dei diritti*, Zanichelli, 2015, p.482 ss.;

POLI, *Logica e razionalità nella ricostruzione giudiziale dei fatti*, in *Rivista di diritto processuale*, 2020, p. 809;

S. PATTI, *sub.* art. 2712 c.c., *Libro sesto: tutela dei diritti art. 2697-2739* in *Commentario del Codice civile e codici collegati Scialoja- Branca- Galgano*, a cura di De Nova, Bologna, 2015, p. 482 ss.;

S.n., *SHA-1 Cryptographic Algorithm*, NIST, 15 December 2022, <https://www.nist.gov/news-events/news/2022/12/nist-retires-sha-1-cryptographic-algorithm> (8/10/2023) ;

VITERBO e CODIGNOLA, *Le macchine di Touring, la legge di Moore e l'uomo bioinformatico*, in *Dir. Informatica*, 2008, p. 321;

VITRANI, *Gli effetti della marcatura temporale nel processo civile*, Giurisprudenza commentata del 27 giugno 2017, in *IUS Processo Telematico*.