valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

Il valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazionale a cura di Marco Scialdone e Telesio Perfetti (Relazione al Convegno del 27 gennaio 2011 - sul Documento informatico)

IL VALORE GIURIDICO DELLE FIRME ELETTRONICHE NELL'ORDINAMENTO GIURIDICO COMUNITARIO E NAZIONALE M. SCIALDONE - T.PERFETTI

1. Premessa: dalla scrittura informatica al documento informatico

Una delle innumerevoli e feconde conseguenze che l'uso generalizzato del computer ha portato seco è stata il dovere per il giurista di interrogarsi nuovamente finanche su concetti dati per acquisiti e, dunque, non necessitanti in apparenza di ulteriori riflessioni.

Si pensi alla scrittura, cui il diritto e la sua evoluzione risultano indissolubilmente legati: scritte, infatti, sono le leggi, le sentenze, gli atti amministrativi, i più importanti negozi giuridici. E' altresì sulla certezza del documento scritto che si fonda una serie innumerevole di rapporti interpersonali e la totalità di quelli tra cittadino e pubblica autorità, al punto che, privato della forma scritta, il diritto avrebbe finito per essere irrimediabilmente diverso da quello che noi oggi conosciamo, con tutta probabilità fondato su pochissimi e generalissimi principi in grado di essere affidati alla memoria e tramandati oralmente (BORRUSO).

Al contrario il diritto e, più in generale, la vita hanno trovato nella scrittura e nei supporti di fissazione della stessa gli strumenti attraverso i quali perpetuarsi, sia pur in un incessante cambiamento segnato dal passaggio delle lastre di pietra, a quelle di bronzo, alle tavolette di argilla, di legno, di cuoio, al papiro, alla pergamena e, solo infine, alla carta.

Ecco, allora, che nell'era del computer ha avuto luogo l'ennesima evoluzione di un concetto che accompagna l'uomo dalla notte dei tempi e ne esprime la volontà di lasciar traccia di sé. Con l'informatica è nato un nuovo modo di scrivere in cui il flusso degli elettroni costituisce il nuovo inchiostro di cui l'uomo si serve; le memorie elettriche o elettroniche la nuova carta, cioè il nuovo supporto; i bit il nuovo alfabeto, universale ed internazionale, di cui l'uomo può servirsi per esprimere qualsiasi opera del pensiero (BORRUSO).

Invero, necessario e sufficiente al concetto di scritto è che si lasci consapevolmente una traccia duratura e, quindi, leggibile tanto al momento in cui la si scrive, quanto a distanza di tempo: il tipo di alfabeto e il supporto usato non contano.

Nonostante ciò, per molto tempo questa possibilità è stata tenacemente negata in dottrina, laddove, identificandosi la scrittura col supporto cartaceo, ci si ostinava a sostenere che la forma elettronica degli atti costituisse un tertium genus rispetto a quella scritta e a quella verbale (GIANNANTONIO), in guisa tale che non potessero assolutamente considerarsi scritti gli atti registrati nelle memorie del computer.

Occorrerà attendere il 1993 per un primo riconoscimento nell'ordinamento italiano della validità giuridica del documento informatico, sia pur limitato all'ambito penale: ci si riferisce alla legge 23 Dicembre 1993, n. 547, recante "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica", con la quale si introduce nel Codice Penale (per quel che qui interessa) l'art. 491-bis. La disposizione in parola, rubricata "Documenti informatici", così disponeva: "Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine, per

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificatamente destinati ad elaborarli".
Solo qualche anno più tardi, nel 1997, si giungerà alla formulazione di quella che sarebbe divenuta la pietra angolare della normativa di settore, ovverosia l'art. 15, comma II, della legge 15 marzo 1997 (la prima "Legge Bassanini"): "Gli atti, dati e documenti formati dalla P.A. e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge".
Come si può notare, la norma richiamava entità disomogenee tanto sotto il profilo della natura giuridica (atti, dati, documenti e contratti), quanto sotto quello dello stadio in cui la rappresentazione informatica veniva in rilievo (formazione degli atti, dati e documenti; conclusione del contratto; trasmissione e archiviazione). Ciò che, invece, accomunava le entità suddette era per l'appunto quello di essere tutte rappresentazioni informatiche (FINOCCHIARO)
La legge veniva seguita dal Regolamento relativo alle modalità e ai criteri per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, il d.P.R. 10 novembre 1997, n. 513 ("Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n.59"), in seguito integralmente trasfuso nel d.P.R. 28 dicembre 2000, n. 445, noto anche come "Testo Unico in materia di Documentazione Amministrativa" (nel seguito, più semplicemente, T.U.D.A.), in cui si enunciava la definizione di documento informatico che è rimasta inalterata attraverso l'evoluzione normativa ed è ora accolta nel D.Lgs. 7 marzo 2005, n. 82 e succ. modif., contenente il nuovo "Codice dell'Amministrazione Digitale" (di seguito, per brevità, CAD): secondo tale definizione il documento informatico è "la rappresentazione informatica di atti, dati, fatti giuridicamente rilevanti".
Con l'informatica è sorto dunque, un nuovo modo di scrivere, il cui alfabeto, costituito dai BIT, dà vita al documento informatico ufficialmente riconosciuto, appellativo da riservarsi dunque al documento formato, elaborato e gestito da sistemi informatici.
Al riguardo non si può fare a meno di notare che, se la l. 547/1993 intendeva originariamente per documento informatico il "supporto" sul quale esso è registrato, nel 1997, più correttamente, lo stesso legislatore ha identificato il documento informatico non più nel supporto, ma nella "rappresentazione informatica di atti, dati, fatti giuridicamente rilevanti": segno evidente di una progressiva assimilazione di una delle verità informatiche in forza della quale esiste una normale scindibilità fisica dei bit registrati su un qualsiasi supporto leggibile a mezzo del computer dal supporto stesso e, dunque, sussiste, altresì, una trasferibilità fisiologica del contenuto del documento informatico da un supporto all'altro, sicché quest'ultimo, non essendo più vincolato alla necessaria incorporazione col primo, finisce col diventare irrilevante rispetto al contenuto stesso[1].
Vedremo in seguito come siffatta caratteristica ponga in crisi la tradizionale contrapposizione tra originale e copia finendo per svuotare di senso la stessa nozione di copia, quale documento di secondo grado.
Quello che si può sin d'ora affermare è che la nozione di documento informatico sopra riportata

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

si pone sulla scia della concezione carneluttiana secondo la quale il documento è “una cosa che fa conoscere un fatto” (CARNELUTTI)[2], in ciò contrapponendosi alla testimonianza. Con il documento, infatti, l’effetto conoscitivo viene realizzato attraverso la tecnica della rappresentazione, ossia il soggetto non ha diretta percezione di un determinato fatto, ma si rappresenta (e conosce) quello stesso fatto attraverso le sensazioni che gli provengono dalla percezione del documento (GRAZIOSI).
In sintesi, nel documento rilevano:
ü il supporto materiale, ossia la res (irrilevante essendo la materia di cui è composta: carta, pietra, pezzo di legno, nastro magnetico, etc.)[3];
ü il “veicolo”, cioè lo strumento tramite il quale un fatto viene rappresentato (per es. la scrittura[4], ma anche un dipinto, un disegno, una fotografia, un ritratto, un nastro magnetico etc.);
ü il contenuto rappresentativo e a tal proposito il documento può avere carattere meramente narrativo, come un documento storico, oppure dichiarativo ed è in tale ultimo caso che esso assume rilevanza per il diritto, in quanto il contenuto attesta quanto fatto o detto dal documentatore; in tal senso esso può avere un contenuto “testimoniale” (pere es. una dichiarazione di scienza come una quietanza) o invece dispositivo ovvero negoziale (per es. una dichiarazione di volontà espressa in un contratto o in un provvedimento).

2. LA FIRMA ELETTRONICA: NOZIONE E TIPOLOGIE
Tematica immediatamente correlata al riconoscimento della rilevanza giuridica del documento informatico è quella della possibilità che esso rechi la sottoscrizione del suo autore, unico e sicuro segno, secondo il nostro ordinamento, della attribuibilità dell'atto a un determinato soggetto (in gradi garantire la “paternità” e dunque la certezza della provenienza del documento) e della volontà di questi di rendersi responsabile del suo contenuto (c.d. “non ripudiabilità” del documento).
Col computer è infatti certamente possibile riprodurre una firma autografa, ma non una sottoscrizione. Basti considerare che tra i suoi organi di input, il computer annovera anche una speciale lavagna elettromagnetica (“graphic tablet”), sulla quale si può liberamente disegnare a mano, sì da consentire in output la riproduzione del disegno per identità d’immagine, in modo tale che la riproduzione appaia assai difficilmente distinguibile dall'originale.
Ma se nel documento cartaceo la riferibilità della firma al suo autore è resa certa dalla stessa fisicità del foglio, contenente, sopra il testo e, sotto, la firma, invece, a mezzo del computer sarebbe estremamente agevole, per chi volesse falsificare un documento, riportare in automatico, in calce a un determinato testo stampato, la firma autografa della persona cui lo si intendesse attribuire, prelevando la firma da un documento originale, realizzando così una sorta di “fotomontaggio elettronico”.
La scienza informatica ha dunque dovuto creare nuove modalità di sottoscrizione del documento (informatico) che fossero in grado di ovviare agli inconvenienti sopra indicati, modalità che potessero servire da “firma” in quanto contraddistinguenti il sottoscrittore per qualcosa che è, che sa o che fa: nasce così il concetto di firma elettronica, ovverosia qualsivoglia marcatura elettronica che indichi l'identità di un soggetto da considerarsi firmatario del documento. Merita a tal proposito menzione quanto riportato nelle “Linee guida per

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

l’utilizzo della Firma Digitale”[5] del CNIPA (oggi DigitPA). Precisamente nel paragrafo intitolato “La firma digitale e la direttiva europea sulle firme elettroniche” si specifica che “la firma elettronica (generica) può essere realizzata con qualsiasi strumento (password, PIN, digitalizzazione della firma autografa, tecniche biometriche, ecc.) in grado di conferire un certo livello di autenticazione a dati elettronici”. Secondo questa lettura della normativa, indicata ufficialmente dal CNIPA nelle Linee Guida, si potrebbero considerare idonei strumenti di autenticazione in grado di attribuire “forma scritta” ai documenti informatici di riferimento, anche se, come si vedrà nel prosieguo della trattazione, liberamente valutabili dal giudice dal punto di vista probatorio:
ü gli accessi in un'area riservata di un sito web al fine di autenticare tutte le future transazioni da effettuare online;
ü le e-mail;
ü la spedizione telematica delle dichiarazioni dei redditi (ENTRATEL del Ministero dell'Economia);
ü alcune sottoscrizioni che avvengono senza smart-card nei processi di e-banking.
La differenza fondamentale che intercorre tra le diverse tipologie di firma elettronica è rappresentata, oltre che dalla tecnologia utilizzata, anche dalla loro maggiore o minore capacità di assicurare la presenza di tutti gli elementi richiesti per garantire la manifestazione di volontà da parte del soggetto firmatario, nonché l'integrità e l’ immodificabilità del documento così firmato.
Al momento la soluzione tecnica in grado di garantire maggiormente la presenza degli elementi da ultimo richiamati è rappresentata da quella particolare tipologia di firma elettronica denominata firma digitale.
La firma digitale è basata su un sistema di chiavi asimmetriche a coppia, pubblica e privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Sulla base della definizione sopra riportata proviamo, ora, a comprendere come funziona la firma digitale, cioè come si può dare ad un documento informatico la certezza sull’identità del firmatario e sull'integrità del contenuto.
Innanzitutto il cifrario asimmetrico: esso è fondato sull'uso di due chiavi diverse, generate insieme nel corso di un unico procedimento. Una delle due chiavi serve per cifrare (chiave diretta) l’altra per decifrare (chiave inversa).
Le proprietà fondamentali di una tale sistema sono:
ü non si può decifrare il testo con la stessa chiave usata per cifrarlo;
ü le due chiavi sono generate con la stessa procedura e correlate univocamente;
ü conoscendo una delle due chiavi non c'è nessun modo di ricostruire l'altra.
In tal modo una delle due chiavi può essere resa pubblica, mentre l'altra deve essere mantenuta segreta.
A questo punto il sistema più elementare per garantire al terzo la provenienza e l'integrità del documento sarebbe quello di inviargli un testo chiaro insieme ad una versione dello stesso cifrata con la chiave privata del mittente. Il destinatario sarebbe chiamato a decifrare il testo con la chiave pubblica del mittente e, se i due testi risultassero uguali, otterrebbe entrambe le

certezze sull'identità del mittente e sull'integrità del contenuto.
Tuttavia un sistema del genere è lento, perché bisognerebbe cifrare e decifrare tutto il documento, operazione che può richiedere molto tempo, in quanto strettamente connessa alle capacità dell'elaboratore utilizzato.
Per ovviare ad un simile inconveniente si ricorre allora a una semplificazione che consiste nel cifrare solo un brevissimo riassunto del testo stesso, ottenuto con una procedura detta funzione di hash: pochi caratteri che costituiscono l'impronta del testo (digest).
Se alla fine della procedura l'impronta che risulta dalla decifratura con la chiave pubblica del mittente è uguale a quella che si ottiene applicando la funzione di hash al testo chiaro, vuol dire che esso proviene da chi appare come il titolare della chiave pubblica e che non è stato alterato dopo la generazione della firma digitale.
Quanto delineato ruota attorno a un perno centrale che è quello della conoscibilità della chiave pubblica, con il corollario della sua attendibilità.
Se la comunicazione deve svolgersi tra due soggetti che si conoscono, essi possono direttamente scambiarsi le rispettive chiavi pubbliche. Ma il grande vantaggio dei sistemi di crittografia a chiave asimmetrica è proprio la possibilità di rendere pubblica una delle due chiavi, consentendo a chiunque di controllare che un messaggio provenga proprio dal titolare dell'altra chiave - quella privata - e che non sia stato alterato o contraffatto (CAMMARATA – MACCARONE)
Naturalmente la pubblicazione e il controllo delle chiavi si svolgono per via telematica, accedendo ad appositi registri, che costituiscono il punto critico del sistema.
Infatti, è indispensabile che i gestori di questi registri siano soggetti assolutamente scrupolosi e fidati e che siano, in qualche modo, a loro volta, certificati. Altrimenti sarebbe assai agevole per un malintenzionato pubblicare una chiave facendosi passare per un altro o contraffare chiavi altrui, con o senza la complicità del gestore del registro, con il risultato che dalla massima sicurezza consentita dalla crittografia a chiave asimmetrica si passi alla massima insicurezza che deriva dalla malafede, o più semplicemente dalla negligenza, aggravate dall'impossibilità di distinguere i bit veri da quelli falsi (CAMMARATA – MACCARONE).
Dunque in tutto il processo della firma digitale è necessario l'intervento di una “terza parte fidata” (trusted third part), generalmente nota come Certification Authority (nel nostro ordinamento “il certificatore”).
Nello schema teorico della firma digitale c'è una distinzione tra CA (Certification Authority) e RA (Registration Authority): la prima ha il compito di gestire il database delle chiavi pubbliche e dei relativi certificati delle chiavi, la seconda ha la responsabilità di procedere all'identificazione del soggetto che richiede la certificazione.
Questo sdoppiamento è stato rifiutato dal legislatore italiano che ha invece optato per l’unificazione dei ruoli ponendo in capo a un unico soggetto (il certificatore) tutte le responsabilità derivanti dall'esercizio della certificazione, con l'evidente vantaggio di offrire al consumatore-utente una maggiore tutela.
L'insieme costituito dai soggetti indicati (utente, certificatore, destinatario ecc.), il modo con il quale ciascuno di essi assolve al proprio ruolo e le modalità di utilizzazione delle tecnologie disponibili, costituisce la c.d. “PKI” (acronimo per Public Key Infrastructure) o infrastruttura a chiave pubblica.

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

Per diversi anni la firma digitale ha rappresentato l'unico strumento previsto nel nostro ordinamento per una sottoscrizione valida ed efficace del documento informatico.
Su tale assetto ha inciso il D.Lgs. 23 gennaio 2002, n. 10, recante la "Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche" e che ha finito per rompere l'originario assetto monopolistico a favore di una pluralità di sottoscrizioni elettroniche del documento informatico; tutto questo in ossequio al principio in essa contenuto volto ad un approccio tecnologicamente neutrale, orientato cioè a una formulazione neutra della disciplina quanto alla tecnologia informatica cui si riferisce, in modo da evitare una prematura obsolescenza della stessa.
Nella direttiva, centrale era la dicotomia "firma elettronica" – "firma elettronica avanzata", attorno alla quale ruotava un sistema "a doppio binario", con l'attribuzione di un diverso e crescente valore giuridico a seconda che il documento informatico fosse sottoscritto con la prima o la seconda tipologia di firma.
In modo coerente con tale impostazione, il legislatore italiano aveva operato la trasposizione nel diritto interno delle definizioni normative di rilievo.
E così l'art. 2, comma 1, lett. a) e lett. g), del D.Lgs. 10 cit., definivano rispettivamente la firma elettronica come "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica, utilizzati come metodo di autenticazione informatica" e la firma elettronica avanzata come "la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati".
Sul piano probatorio, il testo unico sopra richiamato conferiva al documento informatico non sottoscritto l'efficacia probatoria prevista per le riproduzioni meccaniche, di cui all'articolo 2712 c.c., mentre al documento informatico sottoscritto con firma elettronica veniva riconosciuta la capacità satisfattiva del requisito legale della forma scritta restando, in termini probatori, liberamente valutabile dal giudice, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.
Su quest'ultimo punto il CAD, nella sua prima formulazione, aveva segnato un'inversione di tendenza, prevedendo che solo il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale fosse in grado di soddisfare il requisito legale della forma scritta, laddove eguale efficacia era preclusa in caso di sottoscrizione con firma elettronica c.d. "semplice" o "debole": successivamente, con il D.Lgs. 4 aprile 2006, n. 159 (di seguito anche "primo decreto correttivo") in buona sostanza, si è tornati indietro, sia pure con una scelta normativa differente da quella del T.U.D.A.
Attualmente, con l'entrata in vigore del D.Lgs. 30 dicembre 2010, n. 235 (di seguito anche "secondo decreto correttivo"), si è nuovamente ritornati alla previsione della firma elettronica avanzata, con ciò incidendo anche sulla definizione di firma digitale. Infatti nel CAD post primo decreto correttivo erano presenti la firma elettronica, la firma elettronica qualificata e la firma digitale, quest'ultima quale tipo di firma elettronica qualificata. Dopo il secondo decreto si può affermare che allo stato esistono le seguenti forme di firma elettronica:
ü firma elettronica (art. 1, lett. q, del CAD);

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

ü firma elettronica avanzata (art. 1, lett. q-bis, del CAD);
ü firma elettronica qualificata (art. 1, lett. r, del CAD);
ü firma digitale, quale particolare tipo di firma elettronica avanzata e non più qualificata (art. 1, lett. s, del CAD).
Di questi e di altri aspetti si avrà, tuttavia, modo di parlare più approfonditamente nel prosieguo della trattazione.

3. IL DOCUMENTO INFORMATICO NEL CODICE DELL'AMMINISTRAZIONE DIGITALE
Il legislatore del 1942, nella redazione del codice civile, ha dato prevalentemente rilievo a due figure di documento, l'atto pubblico e la scrittura privata: rendere i documenti informatici equipollenti a quelli cartacei per gli effetti costitutivi e probatori, significava ricondurli a tali tipi.
Tuttavia non si può sottacere come, nel campo dei documenti informatici, si possono immaginare molte più tipologie che nei documenti cartacei: la pluralità di firme elettroniche moltiplica la possibilità di "scritture private informatiche" (GENTILI), ponendo all'attenzione dell'operatore del diritto nuove tipologie di documenti che stentano ad essere inquadrate nella tradizionale dicotomia codicistica atto pubblico/scrittura privata.
Il CAD, che raccoglie la normativa in merito, dopo il secondo decreto correttivo riconosce la rilevanza a varie tipologie di documento informatico:
- il documento informatico non sottoscritto;
- il documento informatico munito di firma elettronica c.d. semplice;
- il documento informatico munito di firma elettronica avanzata, qualificata ovvero di firma digitale;
- la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.
Il primo e più semplice tipo che si incontra nel CAD è il documento informatico non sottoscritto.
Come detto in precedenza, nel nuovo corpus normativo è stata confermata la definizione di documento informatico quale "rappresentazione di atti, fatti o dati giuridicamente rilevanti" (art. 1, lett. p, CAD).
Per quel che qui maggiormente interessa occorre riportare subito il dettato dei commi 1-bis dell'art. 20 del Codice che così recitano: "L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità fermo restando quanto disposto dall'articolo 21".
Analizzando la disposizione, appare evidente come l'intento del legislatore sia stato quello di ampliare il novero dei documenti informatici in grado di soddisfare il requisito della forma scritta, un intento ampiamente condivisibile, anche al fine di salvaguardare le prassi riscontrabili nella contrattazione online dettate da esigenze di rapidità e celerità e che non sono incentrate sull'utilizzo della firma digitale.
Almeno in linea teorica, infatti, si riconosce a qualsiasi documento informatico la capacità satisfattiva del requisito della forma scritta, sia pure passando attraverso il vaglio di una valutazione giudiziale ancorata ai parametri normativamente indicati.
Non si può fare a meno di notare tuttavia come il citato comma 1-bis finisca, almeno potenzialmente, per allargare un po' troppo il novero dei documenti informatici idonei a

soddisfare il requisito della forma scritta. E' singolare, infatti, che, nella disposizione da ultimo richiamata, il legislatore abbia omesso di far riferimento ad alcun tipo di sottoscrizione elettronica di cui gli stessi dovrebbero essere dotati per raggiungere una simile finalità: si potrebbe, dunque, immaginare, in astratto, un documento informatico "non firmato" che sia reputato dal giudice in grado di soddisfare il requisito della forma scritta in ragione delle sue oggettive caratteristiche di qualità, sicurezza, integrità e immodificabilità. Ma potrebbe esattamente accadere il contrario e cioè che un documento informatico cui sia stata apposta una firma elettronica semplice non potesse essere reputato in grado di assolvere a quell'obbligo imposto per "gli atti che devono farsi per iscritto" (per riprendere la terminologia utilizzata nella rubrica dell'art. 1350 c.c.). Basta infatti leggere l'art. 21, comma 1, del CAD: "Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità". Pertanto anche dopo l'entrata in vigore del secondo decreto correttivo la svista legislativa non è stata completamente corretta, dal momento che con riferimento al documento sottoscritto con firma elettronica semplice continua ad avere sul piano probatorio la stessa efficacia di quello non sottoscritto e nulla si dispone in ordine al valore formale, forse sottinteso a fortiori (se è idoneo quello non sottoscritto, tantundem quello sottoscritto, ma nulla si stabilisce in ordine al "come" della valutazione, che per forza di cose sarà la medesima)[6]. Di fatto si offre al giudice ampia discrezionalità nel decidere, sia pur sulla base di caratteristiche oggettive del documento (normativamente indicate), se lo stesso sia in grado o meno di soddisfare il requisito della forma scritta.
Una siffatta impostazione potrebbe essere contraria alla stessa ratio insita nella prescrizione formale quale elemento costitutivo del contratto. Del resto il requisito della forma scritta risponde principalmente all'esigenza delle responsabilizzazione del consenso. Questa esigenza si rileva particolarmente in relazione all'onere dell'atto pubblico, che impone alla parte di dichiarare il proprio consenso ad un pubblico ufficiale. Seppure in misura minore anche l'onere della scrittura privata vale a richiamare l'attenzione della parte sulla dichiarazione fatta propria mediante la sottoscrizione (BIANCA).
Ora è pacifico che la sottoscrizione non debba necessariamente essere apposta con una penna, ma possa essere rappresentata da altri segni che egualmente comprovano l'identità della persona e la sua volontà di far propria una dichiarazione (BORRUSO), in particolare sfruttando le prestazioni di cui è suscettibile un computer, per es. adottando opportuni sistemi per il riconoscimento personale del soggetto da cui proviene la dichiarazione. Tuttavia una qualche forma di sottoscrizione dovrebbe pur sempre essere richiesta, proprio per quella funzione di responsabilizzazione del consenso cui sopra si faceva cenno e che è rinvenibile tanto laddove il soggetto apponga la sua firma autografa al documento cartaceo, tanto laddove l'autografia sia sostituita da procedure informatiche intese a far risultare l'identità del dichiarante e la sua volontà di rispondere della dichiarazione medesima.
E' altrettanto vero che, con la soluzione adottata, il legislatore ha voluto legare la normativa generale contenuta nel CAD con quella speciale dedicata alla conservazione sostitutiva dei documenti informatici (si fa riferimento alla Deliberazione CNIPA (oggi DigitPA[7]) n. 11 del 19 febbraio 2004 e al Decreto del Ministero dell'Economia e delle Finanze del 23 gennaio 2004). In quest'ultima, infatti, il concetto di documento informatico valido e rilevante è accostato alle sue

caratteristiche intrinseche di immodificabilità e staticità, anche a prescindere dalla presenza di una sottoscrizione digitale. La sottoscrizione e la firma elettronica, dal punto di vista sistematico, riguarderebbero invece l'ambito probatorio, relativo alla provenienza del documento informatico (che rimarrebbe pur sempre, nella sua essenza, “forma scritta”). Questa evoluzione del concetto della “forma scritta” – legata alla natura del documento informatico e ad una certamente problematica valutazione giudiziale delle sue caratteristiche tecniche – opera, in maniera opportuna, una cesura con il passato: non si sarebbe più in presenza di una condicio sine qua non tra rigida appartenenza del documento informatico a qualcuno attraverso i sistemi della firma digitale e validità formale di quella dichiarazione negoziale.

3.1 IL DOCUMENTO INFORMATICO SOTTOSCRITTO CON FIRMA ELETTRONICA C.D. “SEMPLICE”

Quella della firma elettronica c.d. semplice all'interno del nostro ordinamento è una storia travagliata che ha la sua genesi nella la direttiva 1999/93/CE, laddove era definita come “l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione”. La direttiva veniva poi recepita nell'ordinamento italiano con il D.Lgs. 10/2002, cui seguiva il D.P.R. 137/2003 che ne segnava formalmente l'ingresso nel panorama giuridico nazionale interrompendo il monopolio della firma digitale nell'ambito delle sottoscrizioni elettroniche legalmente riconosciute.

Tuttavia le modalità di recepimento sono state da subito oggetto di severe critiche (CAMMARATA). Si è sottolineato, infatti, come le definizioni della direttiva, nella versione in inglese, fossero formulate in linguaggio tecnico ed avessero un preciso significato in quel contesto, ma che non avessero ricevuto fedele traduzione nelle formulazione italiana (OSNAGHI).

In particolare, la primigenia definizione italiana di firma elettronica aveva impropriamente aggiunto alla parola “autenticazione” l'aggettivo “informatica”, assente nella versione inglese, avendo avvertito il legislatore italiano l'insopprimibile esigenza di aggettivare un sostantivo niente affatto ambiguo nel linguaggio tecnico, ma che avrebbe potuto disturbare il giurista per il quale l'autenticazione è strettamente correlata all'attività del pubblico ufficiale.

La soluzione adottata, tuttavia, non aveva raggiunto il risultato sperato tant’è che non erano mancate le critiche di chi riteneva che, comunque, il termine autenticazione avrebbe dovuto rimanere riservato alle sole operazioni di competenza del pubblico ufficiale (CAMMARATA).

Successivamente, con il primo decreto correttivo è stata apportata una variazione alla definizione di “firma elettronica”, sostituendo l'espressione “autenticazione informatica” con quella di “identificazione informatica”. Allo stato attuale la lettera q) dell'articolo 1, comma I del Codice così recita: “firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica”.

Siffatta modifica, se ha avuto senza dubbio il merito di ovviare alle critiche di cui sopra, ha avuto l'altrettanto innegabile merito di sgomberare il campo sulla natura giuridica della firma elettronica c.d. semplice.

Si era infatti sostenuto in dottrina (CAMMARATA, OSNAGHI) che la firma elettronica semplice servisse esclusivamente a validare dei dati e che, dunque, non sembrasse opportuno definirla

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

“firma”, strumento che, al contrario, ha la doppia funzione di validazione di dati e validazione dell’identità del firmatario. Al contrario, nella relazione illustrativa del primo decreto correttivo è possibile leggere quanto segue: “è stata modificata la definizione di firma elettronica, sostituendo la parola ‘autenticazione’ con la parola ‘identificazione’ sottolineando la circostanza che la firma elettronica ha lo scopo di indicare l’identità del soggetto che sottoscrive il documento”. La nuova definizione, pertanto, impedisce qualsiasi possibilità interpretativa difforme.
Per quanto attiene agli effetti probatori, il primo comma dell'articolo 21, sulla scorta della previsione comunitaria (direttiva 1999/93/CE, art. 5, comma 2) che imponeva agli Stati membri di non considerare inefficace e irrilevante il documento informatico con firma elettronica semplice (pur sempre in virtù del principio di neutralità tecnologica e di “non discriminazione”), ha statuito che lo stesso è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza, integrità ed immodificabilità (da notarsi che questi due ultimi criteri di valutazione sono stati inseriti con il primo decreto correttivo, laddove in precedenza si faceva riferimento esclusivamente alla “qualità” e alla “sicurezza”).
Si rimane sostanzialmente ancorati alla formula contenuta nel T.U. 445/2000 come modificato dal D.Lgs. 10/2002 e, dunque, a un livello di efficacia probatoria difficilmente inquadrabile, peraltro con il rischio di apparire come un'inutile ulteriore gradazione rispetto alle categorie già enucleate nel codice civile e in quello di procedura civile con particolare riferimento alle previsioni di cui agli articoli, rispettivamente, 2712 c.c. e 116 c.p.c.
Quest'ultima disposizione stabilisce, infatti, in linea generale che “il giudice deve valutare le prove secondo il suo prudente apprezzamento salvo che la legge disponga altrimenti”.
Ora non si comprende se quanto previsto dal primo comma dell'articolo 21 del CAD finisca o meno per fornire al giudice istruzioni diverse rispetto a quelle già contenute nell'articolo 116 c.p.c.: peraltro, quale che sia la risposta ad un simile dubbio interpretativo, essa non consentirebbe comunque di sciogliere le riserve sulla formulazione della norma giacché in caso affermativo sarebbe necessario individuare i parametri da tenere in considerazione, mentre, in caso negativo, ingenererebbe problemi interpretativi in relazione al richiamato art. 116 c.p.c.
Volendo entrare nella discrezionalità con la quale il giudice sarà chiamato a valutare il documento di cui trattasi di sicuro andranno prese in considerazione le peculiari caratteristiche tecniche, di volta in volta riscontrabili, in grado di avvicinare la firma elettronica “semplice”, oggetto di esame, alla firma elettronica avanzata e qualificata.
Si pensi, per es., al caso in cui la prima possegga le caratteristiche tecniche che la legge richiede per le seconde, ma non l'attribuzione da parte di un certificatore: in una simile ipotesi sarà ragionevole valutare credibili il testo e la sottoscrizione in sé e domandarsi solo se sia altrettanto ragionevole anche il collegamento all'identità cui la firma riconduce. Tutto dipende, dunque, nella circostanza oggetto di valutazione, da cosa sia l'insieme di dati in forma elettronica usati per firmare, e quale e quanto resistente sia la loro connessione ai dati elettronici che compongono il testo.
C’è, però, un ulteriore aspetto del richiamato art. 21 cit. che merita di essere sottolineato, in quanto potenzialmente in grado rendere il documento informatico provvisto di firma elettronica, per certi versi, più forte di quello cartaceo munito di sottoscrizione. La scrittura privata convenzionale se disconosciuta perde la virtù probatoria, salva verificazione. Il documento

informatico con firma elettronica semplice, invece, potrebbe anche mantenerla. Così mentre agli effetti sostanziali la sua rilevanza parrebbe diminuita, ne risulterebbe aumentata a quelli probatori.
A completamento di quanto sopra scritto in materia di firma elettronica semplice o debole, merita menzione l'art. 4, comma 4, del D.P.C.M. 6 maggio 2009, recante le "Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini"[8], che dispone come segue: "L'invio tramite PEC costituisce sottoscrizione elettronica ai sensi dell'art. 21, comma 1, del decreto legislativo n. 82 del 2005".

3.2 IL DOCUMENTO INFORMATICO SOTTOSCRITTO CON FIRMA ELETTRONICA AVANZATA, QUALIFICATA O DIGITALE
Il documento informatico munito di firma digitale, che oggi costituisce, lo si ripete, una species di firma elettronica avanzata, è oggetto di minuziosa disciplina da parte dell'ordinamento, tale da vincolarne la natura prima ancora che il valore (GENTILI).
Si rinvia a quanto esposto in premessa per gli aspetti squisitamente informatici.
Orbene sul piano definitorio è importante ricordare quanto segue:
ü la firma elettronica avanzata è l'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario (c.d. "entity authentication", ottenuta grazie al certificato in cui sono registrati i dati del titolare), creati con mezzi sui quali il firmatario può conservare un controllo esclusivo (esistenza di un supporto hardware, come un dispositivo USB, una smart-card o un token), collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (data authentication);
ü la firma elettronica qualificata è un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
ü la firma digitale infine è un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Rispetto alla precedente formulazione (quella antecedente secondo decreto correttivo, ove la firma digitale era considerata una particolare forma di firma qualificata) si perde, a livello definitorio, il riferimento della firma digitale al c.d. "dispositivo sicuro" di firma[9] (tipico della firma qualificata e non di quella avanzata), contenuto solo nella definizione di firma elettronica qualificata. Inalterate rimangono le definizioni di chiave privata e chiave pubblica, nonché di certificato qualificato, tutti connessi alla firma digitale che, pertanto, già a livello definitorio, continua ad essere l'unico tipo di firma elettronica legata ad una determinata tecnologi (ROGNETTA).
Con particolare riferimento dunque alla firma digitale, essa ex art. 24 del CAD deve riferirsi in maniera univoca ad un solo soggetto e al documento o all'insieme di documenti cui è apposta o associata; per la sua generazione occorre adoperare un certificato qualificato che, al momento

della sottoscrizione, non risulti scaduto, revocato o sospeso. Attraverso tale certificato devono rilevarsi la sua validità, gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.
Da tali disposizioni emerge con chiarezza quel passaggio epocale che la firma digitale ha già in parte determinato e sempre più contribuirà a determinare: mentre la firma autografa di un individuo è sempre uguale a se stessa, la firma digitale è sempre diversa, perché viene di volta in volta generata a partire dal contenuto del documento. Si può dire che mentre la firma autografa è orientata all'individuo, la firma digitale è orientata al documento.
Questo innesca dinamiche giuridiche del tutto nuove, prima fra tutte l'esigenza di un soggetto, terza parte fidata (leggasi: il certificatore), che attesti la nostra identità, attesti in sostanza “chi siamo”. Mentre nei sistemi tradizionali di firma è la calligrafia a farsi portavoce e garante della nostra identità, il carattere inevitabilmente neutro dei bit pone un'esigenza ulteriore che è quella legata all'identificazione del soggetto firmatario.
Attualmente il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche previste dal CAD medesimo che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia probatoria prevista dall'art. 2702 c.c. Inoltre l'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.
Ne consegue che siffatto documento è a tutti gli effetti la “scrittura privata informatica”, di cui, nei rapporti online, interpreta il ruolo e riproduce tendenzialmente la disciplina, sia pure con i doverosi adattamenti dovuti alla natura del mezzo.
Un primo adattamento attiene al profilo temporale: la firma digitale opera in regime di durata limitata e ciò determina, altresì, una limitazione della sua efficacia sostanziale. Essa vale a trasformare in scrittura privata il documento informatico cui è associata, solo se il relativo certificato di firma non è scaduto, revocato o sospeso all'atto della sottoscrizione (GENTILI).
A ciò aggiungasi che il certificato da ultimo richiamato può contenere l'indicazione di determinati limiti d’uso e/o di valore, o ancora le qualifiche specifiche del titolare, quali l’appartenenza a ordini o collegi professionali, la qualifica di pubblico ufficiale, l’iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza.
Tutti fattori, quelli testè citati, in grado di incidere sul valore giuridico della sottoscrizione. Con i limiti di uso, infatti, il certificato sottrae alla firma il valore di sottoscrizione giuridicamente impegnativa, sottraendo, a sua volta, al documento informatico cui è apposta la capacità di soddisfare il requisito della forma scritta. Con i limiti di valore, invece, imprime le stesse restrizioni in relazione al valore economico degli atti unilaterali o dei contratti sottoscritti con quella firma digitale. (GENTILI).
Per quanto attiene all'efficacia probatoria, essa è stata più volte oggetto di rivisitazione da parte del legislatore: si ritiene, pertanto, opportuno operare un excursus storico sì da meglio comprendere l'attuale disciplina.
Il D.P.R. 513/97 ed il d.P.R. 445/2000, prima del recepimento della direttiva 1999/93/CE, riconoscevamo all'ipotesi del documento informatico munito di firma digitale l'efficacia della scrittura privata di cui all'art. 2702 c.c.; successivamente al recepimento della Direttiva comunitaria, era stata attribuita allo stesso la piena efficacia probatoria fino a querela di falso. In pratica era come se un tale documento fosse stato riconosciuto dalla persona che l'avesse

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

prodotto o, per altri versi, come se godesse della fede pubblica: infatti, chi avesse voluto disconoscerlo avrebbe dovuto proporre querela di falso e fornire le necessarie prove. Diversamente, nel caso della disciplina originaria, in assenza di riconoscimento, era sempre possibile il mero disconoscimento da parte del ritenuto autore, determinandosi così la necessità per chi avesse sostenuto la legittimità della provenienza del documento di fornire adeguata prova (anche attraverso il c.d. processo di verificazione di cui agli articoli 216 e segg. c.p.c.).
La ragione per la quale era stata riconosciuta questa maggiore efficacia risiedeva proprio nel fatto che in tema di firma elettronica sarebbe stato impossibile procedere alla cd. “verificazione” (NEIROTTI): quest'ultima infatti è, per l'appunto, il mezzo di prova mediante il quale una parte chiede di accertare l'autenticità della scrittura o della sottoscrizione di una scrittura privata, dopo che questa è stata disconosciuta dalla controparte, indicando le scritture che possono servire di comparazione (NEIROTTI).
Si intuisce che il carattere necessariamente neutro dei bit rende impossibile qualsiasi comparazione tra documenti informatici i quali nulla porteranno con sé di idoneo ad identificare il loro autore. Mentre per il documento cartaceo la calligrafia è in grado di fornire informazioni su chi lo ha materialmente redatto o sottoscritto (anche tramite l'ausilio di scritture di comparazione o dell'intervento di un consulente tecnico ai fini della c.d. perizia calligrafica), nulla di tutto questo è possibile con riferimento al documento informatico.
Ben si comprende, allora, per quale ragione, modificando l'originaria scelta legislativa, si era deciso di conferire maggiore forza probatoria al documento informatico sottoscritto con firma digitale (o con un altro tipo di firma elettronica qualificata) ponendo a carico del titolare di un certificato firma l'onere della prova circa il disconoscimento di una firma falsa basata sul proprio certificato (NEIROTTI).
Come scritto in precedenza, l’art. 21, comma 2, del CAD dispone che non solo il documento informatico, sottoscritto con firma digitale, ma anche quello sottoscritto con firma elettronica avanzata (quest’ultima ora prevista grazie alle modifiche del secondo decreto correttivo) e qualificata (già presente nella versione antecedente al secondo decreto correttivo) ha l’efficacia prevista dall’articolo 2702 c.c. e che l’utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia la prova contraria. L’efficacia probatoria è dunque equivalente a quella tipica della scrittura privata: quindi efficacia fino a querela di falso soltanto nel caso di riconoscimento da parte dell’autore, rectius del titolare del dispositivo sicuro di firma.
Peraltro, il legislatore ha voluto fornire un elemento aggiuntivo, rispetto alla tradizionale disciplina codicistica, al fine di meglio chiarire come potrebbe avvenire il processo di disconoscimento, e quindi di verificazione giudiziale, stabilendo un principio di presunzione juris tantum di utilizzo del dispositivo sicuro di firma. Ciò per evitare di gravare la parte che produce il documento – poi disconosciuto – di un onere probatorio eccessivamente gravoso, se non impossibile.
La presunzione di utilizzo del dispositivo sicuro di firma opera, dunque, a favore di chi produce in giudizio la scrittura privata, o meglio il documento informatico sottoscritto con firma avanzata, qualificata o digitale, nel senso che dispensa quest’ultimo dall’onere di provare che è stato effettivamente il titolare ad utilizzare materialmente il dispositivo sicuro di firma al fine di effettuare la sottoscrizione elettronica. Nello stesso tempo opera anche a favore del medesimo titolare, nella misura in cui gli consente di liberarsi degli effetti di un utilizzo abusivo di tale

dispositivo di firma dando prova, con qualsiasi mezzo, che l'utilizzo non è a lui riconducibile (NEIROTTI).
Si deve notare che la forza e il pregio della soluzione adottata risiedono proprio nell'interessante bilanciamento degli interessi in gioco che è stato operato, laddove si è sgravata la parte che produce il documento informatico in giudizio di una prova "diabolica", l'utilizzo del dispositivo sicuro da parte del suo titolare, mentre si è garantita al titolare medesimo la possibilità di liberarsi subito degli effetti ingiusti e pregiudizievoli di un utilizzo abusivo, semplicemente fornendo prova contraria, senza nemmeno dover proporre querela di falso.
Pur apprezzando la soluzione tecnica adottata, che realizza quel contemperamento di interessi sopra enunciato, va comunque sottolineato quanto forte rimanga l'esigenza di una modifica alle disposizioni del codice di procedura civile al fine di dettare una peculiare disciplina per il disconoscimento della sottoscrizione digitale e per la querela di falso qualora riguardino un documento informatico, stanti le rilevanti differenze ontologiche tra tale tipologia documentale e quella tradizionale sottoscritta in modo autografo.
Del resto, sul punto fortissime sono state le critiche espresse dal Consiglio di Stato, nell'adunanza del 30 gennaio 2006, nel parere reso sull'allora schema del primo decreto correttivo.
In quella sede il Consiglio di Stato aveva avuto modo di far notare come, con riferimento alla firma digitale (o altro tipo di firma elettronica qualificata), ci fosse una discrasia tra quanto previsto dalla direttiva 1999/93/CE e quanto era stato poi normato nell'ordinamento nazionale al fine di dare attuazione alla suddetta direttiva.
Partendo dalla considerazione che nell'ordinamento italiano, la firma elettronica avanzata, descritta nella direttiva comunitaria, coincide, sul piano tecnico e giuridico, col sistema di firma digitale descritto nel Codice, il Consiglio di Stato ha rilevato come la norma comunitaria imponesse agli Stati membri, quanto agli effetti probatori, esclusivamente di equiparare alla sottoscrizione autografa una firma elettronica avanzata, basata su un certificato qualificato e generata con un dispositivo sicuro e non, dunque, di attribuire ad essa, addirittura, un'efficacia probatoria maggiore.
Si legge nel parere di cui sopra:
«La direttiva non prevede (…) che le firme elettroniche possano conferire al documento informatico una efficacia probatoria maggiore di quella che assume, nel processo, una scrittura privata munita di sottoscrizione autografa.
Il testo risultante dalle modifiche introdotte dal decreto integrativo – invece – rafforza, particolarmente sotto il profilo probatorio, il valore legale del documento informatico sottoscritto con firma digitale a scapito del documento formato sul tradizionale supporto cartaceo.
Le norme del decreto legislativo (che sono soprattutto norme di recepimento, nella specifica materia, delle disposizioni comunitarie) non sembrano recepire correttamente il diritto comunitario nel diritto interno e, soprattutto, sembrano alterare il sistema delle prove nel processo civile.
Com'è noto, nell'intento di non stravolgere il delicato equilibrio del sistema delle prove documentali del processo civile, collaudato da secoli di cultura giuridica, l'articolo 4 del d.P.R. n. 513 del 1997 attribuiva al documento informatico, sottoscritto con firma digitale, "L'efficacia

di scrittura privata ai sensi dell'art. 2702 del codice civile", semplicemente equiparando al documento scritto, sottoscritto con firma autografa, il documento scritto su supporto informatico sottoscritto con firma digitale.
In altri termini, come dalla sottoscrizione autografa si ricava la presunzione di legge, sino a prova contraria, del consenso del firmatario sul contenuto del documento, così dalla sottoscrizione del documento informatico, mediante la firma digitale, l'ordinamento dovrebbe trarre le medesime presunzioni legali, identificando nell'autore della firma digitale l'autore del documento informatico a cui attribuire gli effetti dell'atto.
Nel testo del decreto correttivo, invece, la parità di condizioni è soltanto apparente, poiché l'efficacia probatoria della scrittura informatica è rafforzata dalla maggiore difficoltà del disconoscimento giudiziale della firma (artt. 214 e ss. c.p.c.)
Sostenere che l'uso dello strumento di firma "si presume riconducibile al titolare" e che soddisfa "comunque" il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350 c.c., equivale, in sostanza, ad introdurre nell'ordinamento una presunzione di riconoscimento della provenienza del documento simile a quella prevista dall'art. 2703 c.c. per gli atti formati dal pubblico ufficiale (la firma, per così dire, "si ha per riconosciuta" anche se essa non è stata apposta davanti al pubblico ufficiale).
Pertanto, mentre colui contro il quale viene esibita in giudizio una falsa scrittura cartacea può limitarsi a disconoscere la propria firma dando luogo alla speciale procedura di verificazione prevista dagli artt. 214 e ss. c.p.c. (nella quale è colui che intende utilizzare la scrittura che deve provarne la autenticità), la parte processuale, contro la quale viene esibita in giudizio una falsa scrittura formata su supporto informatico, oltre a disconoscere la propria firma deve anche fornire le prove della sua falsità, con un'inversione dell'onere probatorio che appare ingiustificato.
Si consideri, inoltre, che mentre le prove di una falsa sottoscrizione autografa consistono, di norma, nella produzione di scritture di comparazione, provenienti da atti sottoscritti, ad esempio, in presenza del pubblico ufficiale che li ha autenticati (atti che possono trovarsi nella piena disponibilità della parte, che può, così, tempestivamente esibirli al giudice), nell'ipotesi della firma digitale il reperimento delle prove della falsità della firma costituisce attività più complessa, rendendo ingiustamente oneroso l'esercizio del diritto di difesa da parte del soggetto che lamenta un tentativo di illecita locupletazione ai suoi danni.
Nei casi in cui la falsità consista nell'uso abusivo dello strumento di firma, ad esempio, potrebbe rendersi necessario identificare il calcolatore che è stato utilizzato per formare il documento, la chiave privata utilizzata per apporre la firma, il percorso seguito dal documento trasmesso per via telematica, la validità del certificato emesso dal soggetto certificatore ed altre simili attività. Ciò non significa, evidentemente, che il disconoscimento della firma digitale sia impossibile, bensì che tale attività implica il ricorso a tecniche d'istruzione differenti (ad esempio: il perito grafico sarà sostituito da un perito informatico).
In ogni caso: la diversa natura delle indagini istruttorie per l'accertamento della autenticità del documento certamente non giustifica l'inversione dell'onere della prova a danno di colui che può essere vittima di una macchinazione (né una sostanziale elusione degli obblighi imposti dalla direttiva del 1999).
In conclusione, il documento informatico, munito di firma digitale, sembra porsi, per effetto

dell’inversione dell’onere della prova in tema di disconoscimento, come una sorta di tertium genus tra la scrittura privata e l’atto pubblico, avendo in giudizio la stessa efficacia probatoria di una scrittura privata munita di sottoscrizione legalmente riconosciuta, ed essendo, in realtà, in nulla diverso da una scrittura privata munita di sottoscrizione non autenticata».
Si prende atto che il Legislatore, sul punto, non abbia ritenuto di dar seguito alle critiche mosse dal Consiglio di Stato e, dunque, non abbia ritenuto di tornare all'efficacia probatoria prevista dal D.P.R. 513/1997, addossandosi di fatto il rischio di un eccesso di delega in violazione dell’art. 76 Cost. Ad ogni modo la scelta adottata, ferme restando le lucide argomentazioni suesposte, non appare priva di una certa logicità, come si è cercato di evidenziare in precedenza.
Resta infine da far presente che la superiore dignità della firma digitale e di quella qualificata (equiparate sul piano probatorio alla firma avanzata) riemerge sul piano “formale” nel nuovo comma 2-bis dell’art. 21, introdotto dal secondo decreto correttivo, in base al quale “le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale”. In siffatte ipotesi è la legge e non il giudice a conferire un valore al documento informatico (evidente la differenza rispetto a quello non sottoscritto o sottoscritto con firma elettronica semplice o avanzata). Viene comunque fatta salva dalla disposizione de qua quanto previsto dall’art. 25 del CAD, come novellato dal secondo decreto correttivo, in materia di firma elettronica (quale che essa sia) autenticata da notaio o altro pubblico ufficiale rogante. Ma di ciò ci si occuperà nel paragrafo successivo.

3.3 IL DOCUMENTO INFORMATICO CON FIRMA AUTENTICATA
L’Art. 25, comma 1, del CAD, prevede che si abbia per riconosciuta, ai sensi dell'articolo 2703 c.c., la firma elettronica o qualsiasi altro tipo di firma avanzata[10] autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato. Prosegue il comma 2: “L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico”.
Alcune considerazioni sulla disciplina sopra esposta si impongono. Anzitutto, prima dell’entrata in vigore del secondo decreto correttivo, l’autenticazione era riferita solo alla firma qualificata e a quella digitale (previa verifica del relativo certificato da parte del notaio). Adesso invece è stata allargata l'area delle firme autenticabili, sganciandole dalla necessaria sussistenza di un certificato qualificato o addirittura da qualsivoglia certificato elettronico. La nuova autenticazione può dunque riguardare qualsiasi firma elettronica, inclusa l'acquisizione digitale della sottoscrizione autografa. In dottrina (ROGNETTA) si è fatto notare che il nuovo art. 52-bis della L.16 febbraio 1913, n. 89 (“Ordinamento del Notariato e degli Archivi Notarili”, nota anche come “legge notarile”), come introdotto dal D.Lgs. 2 luglio 2010, n. 110 (“Disposizioni in materia di atto pubblico informatico redatto dal notaio, a norma dell'articolo 65 della legge 18 giugno 2009, n. 69”) ha già previsto che la parti possano sottoscrivere l'atto pubblico informatico, in presenza del notaio, anche con una semplice firma elettronica consistente nell'acquisizione digitale della sottoscrizione autografa (sul punto si tornerà nel prosieguo della

trattazione).
Per quel che poi concerne l'autenticazione da parte del pubblico ufficiale, a differenza del documento cartaceo, non è limitata all'attestazione da parte del pubblico ufficiale che la firma è stata apposta in sua presenza dal titolare previo accertamento dell'identità, ma è estesa alla validità del certificato rilasciato al titolare della firma e, soprattutto, al fatto che il documento non sia in contrasto con l'ordinamento giuridico.
E' interessante ricordare che una prima stesura della norma in commento prevedeva, altresì, che il pubblico ufficiale fosse chiamato ad accertare la conformità del documento alla volontà delle parti. Una statuizione in aperto contrasto col principio di cui all'articolo 2703 c.c., in forza del quale il pubblico ufficiale, quando attesta che la sottoscrizione è stata apposta in sua presenza, non accerta alcunché in relazione alla volontà dell'atto contenuto nel documento sottoscritto.
Come ha avuto modo di affermare il Consiglio di Stato, nel parere citato in precedenza, "l'accertamento del fatto che l'atto corrisponde alla volontà delle parti e che non è in contrasto con l'ordinamento giuridico è un accertamento che la legge devolve alla competenza del notaio (art. 47, comma 3, l. 89/1913 cit.: "Spetta al notaro soltanto d'indagare la volontà delle parti e dirigere personalmente la compilazione integrale dell'atto"), ma solo quando si tratta di atto del quale il notaio cura la redazione, formato a sua cura (atto pubblico), non anche quando si tratta di atto formato dalle parti, la cui sola sottoscrizione sia autenticata".
"Il notaio", prosegue il Consiglio di Stato, "per l'efficacia privilegiata della scrittura autenticata, corrispondente a quella dell'atto notarile stricto iure, è tenuto a controllare che la scrittura non sia contraria all'ordine pubblico (art. 28 legge notarile: per esempio, che non si costituisca un'associazione sovversiva), ma va escluso che sussista l'obbligo del notaio di accertare la corrispondenza del contenuto dell'atto all'effettiva volontà delle parti, obbligo che sussiste solo in caso di atto pubblico".
Dalla versione finale della norma è stato, dunque, saggiamente eliminato ogni riferimento all'indagine sulla reale volontà delle parti che il pubblico ufficiale avrebbe dovuto operare, mentre meglio sarebbe stato sostituire l'espressione "in contrasto con l'ordinamento giuridico" con "in contrasto con l'ordine pubblico" così come suggerito dal Consiglio di Stato.

3.4 I CASI PREVISTI DA DISPOSIZIONI LEGISLATIVE O REGOLAMENTARI NEI QUALI E' OBBLIGATORIO L'USO DELLE FIRMA DIGITALE O COMUNQUE DI ALTRE FORME DI SOTTOSCRIZIONE ELETTRONICA
Nel presente paragrafo verranno indicate, pur senza addentrarsi nel dettaglio delle singole discipline settoriali, le ipotesi espressamente previste da disposizioni legislative o regolamentari, che impongono ai privati o alle P.A. l'uso della firma digitale per la sottoscrizione di documenti informatici giuridicamente rilevanti. Di seguito l'elencazione in ordine cronologico:

Processo civile telematico
Le basi normative del processo civile telematico o "PCT" sono contenute nel d.P.R. 13 febbraio 2001 n.123, "Regolamento recante disciplina sull'uso degli strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei Conti" e nel decreto del Ministero della Giustizia 17 luglio 2008, "Regole tecnico-

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

operative per l'utilizzo di strumenti informatici e telematici nel processo civile"[11]. Il d.P.R. 123/2001 ha istituito il c.d. Sistema Informatico Civile o "SICI" strutturato con modalità tali da assicurare:
a) l'individuazione dell'ufficio giudiziario e del procedimento;
b) l'individuazione del soggetto che inserisce, modifica o comunica l'atto;
c) l'avvenuta ricezione della comunicazione dell'atto;
d) l'automatica abilitazione del difensore e dell'ufficiale giudiziario.
Al SICI possono accedere attivamente soltanto i difensori delle parti e gli ufficiali giudiziari per le attività rispettivamente consentite dal d.P.R. 123/2001. In particolare l'art. 4 del d.P.R. 123/2001 stabilisce che tutti gli atti e i provvedimenti del processo possono essere compiuti come documenti informatici sottoscritti con firma digitale. L'art. 5 del d.P.R. 123/2001 prevede che il processo verbale può essere redatto come documento informatico sottoscritto con firma digitale da chi presiede l'udienza e dal cancelliere. Nei casi in cui è richiesto, le parti e i testimoni procedono alla sottoscrizione delle dichiarazioni o del verbale apponendo la propria firma digitale.
L'art. 6 regolamenta le comunicazioni con biglietto di cancelleria e le notificazioni per via telematica (quest'ultime devono essere sottoscritte con firma digitale), che possono avvenire sia tramite SICI sia all'indirizzo di posta elettronica del difensore, che è unicamente quello comunicato dal medesimo al Consiglio dell'ordine.
Gli artt. 9, 10 e 11 disciplinano gli atti introduttivi del giudizio quali la costituzione, il deposito, la procura alla liti, l'iscrizione a ruolo. Orbene, se la procura alle liti è stata conferita su supporto cartaceo, il difensore, che si costituisce per via telematica, trasmette la copia informatica della procura medesima, asseverata come conforme all'originale mediante sottoscrizione con firma digitale. D'altra parte la nota di iscrizione a ruolo può essere trasmessa per via telematica come documento informatico sottoscritto con firma digitale.
Per quel che concerne il fascicolo informatico d'ufficio, esso è formato dalla cancelleria e contiene gli atti del processo come documenti informatici ovvero le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo. Nel fascicolo informatico sono inseriti anche i documenti probatori offerti in comunicazione o prodotti dalle parti o comunque acquisiti al processo.
Anche la sentenza o la minuta delle medesima (sottoscritta con firma digitale) avviene per via telematica. Il cancelliere, ai fini del deposito della sentenza ai sensi dell'art. 133 c.p.c. sottoscrive la sentenza stessa con la propria firma digitale.
In sintesi la nuova infrastruttura tecnologica serve a eseguire operazioni quali il deposito di atti e documenti, la trasmissione di comunicazioni e notificazioni, la consultazione dello stato dei procedimenti risultanti dai registri di cancelleria, nonché dei fascicoli e della giurisprudenza, operando on line senza la necessità di recarsi fisicamente presso le cancellerie.
Per quel che concerne la figura del difensore delle parti, egli è qualificato come "soggetto abilitato esterno privato"[12] al SICI e ai fini dell'accesso al SICI stesso deve "autenticarsi" (ossia identificarsi in rete, farsi riconoscere online, per es. tramite C.N.S. o altro dispositivo crittografico dotato di certificato digitale) presso il c.d. "punto di accesso" (di seguito, per brevità, p.d.a.). Quest'ultimo è la struttura tecnico-organizzativa che fornisce ai soggetti abilitati esterni i servizi di connessione al gestore centrale[13] e di trasmissione telematica dei

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

documenti informatici relativi al processo, nonché la casella di posta elettronica certificata, peraltro assolutamente dedicata al PCT, tant'è che essa assume la denominazione di "CPECPT" (acronimo per "Casella di Posta Elettronica Certificata per il Processo Telematico). Tutti i collegamenti per la consultazione, per l'invio e il deposito di atti, avviene attraverso il p.d.a. al quale si è iscritti. La consultazione via web delle informazioni contenute nei registri dei procedimenti è realizzato attraverso il sistema "PolisWeb", sistema informatico di consultazione dei Registri di cancelleria dei Tribunali.
Recentemente presso i Tribunali più importanti (incluso quello di Roma) si sta sperimentando il c.d. "decreto ingiuntivo elettronico".
Per esemplificare:
§ viene predisposto il fascicolo di parte in forma elettronica, dove i documenti cartacei vengono digitalizzati;
§ il difensore predispone l'atto mediante l'utilizzo di un redattore, lo imbusta elettronicamente ed appone la propria firma digitale;
§ il difensore si collega al p.d.a. e si autentica dalla sua postazione previo inserimento della propria smart-card in apposito device esterno al proprio computer connesso ad internet; il p.d.a., ad autenticazione avvenuta, dà la possibilità all'utente, di verificare l'elenco degli uffici giudiziari abilitati;
§ una volta scelto l'ufficio giudiziario abilitato, l'utente può consultare le informazioni di suo interesse ed inviare telematicamente la busta su canale sicuro eliminando inutili attese alla cancelleria ed inutili trasferimenti; la busta transita attraverso il gestore centrale che emette l'attestazione temporale di avvenuto deposito;
§ il sistema produce copia cartacea del materiale depositato dal difensore;
§ il magistrato, attraverso la consolle, studia il fascicolo informatico e predispone il provvedimento in formato elettronico, lo firma digitalmente e lo deposita telematicamente in cancelleria;
§ il professionista dalla sua postazione online preleva e deposita la documentazione di suo interesse.

Invio telematico dei bilanci di esercizio delle società
Il D.M. 20 marzo 2003 (in G.U. n. 75 del 31 marzo 2003), rubricato "Sperimentazione dell'invio di bilanci e altri atti rilevanti delle aziende agli organi camerali (CCIAA)" ha autorizzato sino al 30 giugno 2003, il deposito per via telematica o su supporto informatico dei bilanci di esercizio e situazioni patrimoniali, secondo le "Indicazioni tecniche" contenute nell'Allegato al medesimo decreto. L'obbligo di deposito della copia del bilancio e degli atti previsti dall'art. 2435 c.c., veniva validamente adempiuto qualora i documenti trasmessi all'ufficio del registro delle imprese in via telematica, fossero sottoscritti con la firma digitale di un amministratore, il quale garantisce la conformità dei documenti informatici agli originali trascritti e sottoscritti sui libri sociali e conservati per dieci anni. Se poi a siffatto adempimento avesse provveduto un soggetto individuato nella convenzione stipulata con la camera di commercio per la trasmissione delle pratiche per via telematica, alla firma digitale dell'amministratore doveva

essere associata, sul modello di deposito, la firma digitale del soggetto che avesse provveduto alla trasmissione.

Assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto
Il D.M.E.F. 23 gennaio 2004 ha disciplinato in maniera unitaria la procedura informatica relativa all'emissione, alla conservazione e all'esibizione dei documenti rilevanti ai fini fiscali. Le disposizioni del decreto si applicano alle scritture contabili, ai libri, ai registri e, in generale, ad ogni documento fiscalmente rilevante, fatta eccezione per le scritture e i documenti rilevanti ai fini delle disposizioni tributarie nel settore doganale, delle accise e delle imposte di consumo di competenza dell'Agenzia delle dogane.
Come chiarito dall'Agenzia delle Entrate con la circolare del 6 dicembre 2006, n. 36, fra i documenti fiscalmente rilevanti che ricadono nell'ambito di applicazione del decreto sopra citato possono annoverarsi, a titolo esemplificativo: il libro giornale e il libro degli inventari, le scritture ausiliare nelle quali devono essere registrati gli elementi patrimoniali e reddituali, le scritture ausiliarie di magazzino, il registro dei beni ammortizzabili, il bilancio di esercizio, i registri prescritti ai fini dell'imposta sul valore aggiunto.
I documenti informatici rilevanti ai fini tributari devono essere statici e non modificabili[14]: essi, pertanto, non devono contenere macroistruzioni[15] o codici eseguibili[16].
Ai sensi dell'art. 3, comma 1, lett. b), del D.M.E.F. cit., il documento informatico deve essere emesso, al fine di garantirne l'attestazione della data, l'autenticità e l'integrità, con l'apposizione del riferimento temporale e della sottoscrizione elettronica.
Per riferimento temporale si intende un'informazione che associa al documento la data e l'ora. A più documenti può essere applicato il medesimo riferimento temporale.
Per sottoscrizione elettronica s'intende l'apposizione al documento informatico della firma elettronica qualificata.
Recentemente è inoltre intervenuta l'Agenzia delle Entrata con un provvedimento attutivo della comunicazione dell'impronta relativa ai documenti informatici rilevanti ai fini tributari, ai sensi dell'art. 5, comma 2, del D.M.E.F. 23 gennaio 2004[17]. Il provvedimento contiene le istruzioni che il c.d. "il responsabile della conservazione" (v. punto successivo) dei file dovrà seguire per trasmettere telematicamente all'Agenzia l'impronta digitale dell'archivio informatico dei documenti fiscalmente rilevanti, con riferimento ai periodi d'imposta 2010 e precedenti. La comunicazione deve essere inviata esclusivamente tramite il canale Entratel o Fisconline e deve contenere, tra le altre informazioni, i dati identificativi dell'interessato, del responsabile della conservazione o del suo eventuale delegato, l'elenco dei documenti cui si riferisce l'impronta, l'indicazione del luogo in cui è conservata l'evidenza informatica da cui è stata generata l'impronta, la marca temporale apposta all'archivio.
In via generale, i contribuenti che creeranno l'archivio informatico dei documenti relativi al 2010 dovranno comunicarne l'impronta entro gennaio 2012.
Per gli anni d'imposta precedenti al 2010, i contribuenti che hanno proceduto a conservare i documenti rilevanti ai fini tributari con modalità digitale dovranno trasmettere le comunicazioni sempre entro gennaio 2012, ossia entro lo stesso termine d'invio previsto per comunicare l'impronta dell'archivio informatico relativo al 2010. La comunicazione all'Agenzia delle

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

Entrate estende la validità dei documenti fino a che permane l’obbligo di conservarli ai fini tributari.

Conservazione sostitutiva
Legato strettamente al concetto di documento informatico è quello di dematerializzazione. In tal sede siffatto argomento merita la spendita di qualche considerazione in più.
Per dematerializzazione si intende la progressiva sostituzione della documentazione cartacea con i documenti informatici ottenuta tanto attraverso la promozione dell'uso del computer quale strumento privilegiato di redazione degli atti giuridicamente rilevanti, quanto attraverso la progressiva digitalizzazione dei documenti analogici esistenti.
Numerosi sono stati i provvedimenti normativi che nel corso degli anni hanno consentito la piena sostituibilità dell'archivio cartaceo con l'archivio digitale. A tal proposito si ricorda che una delle prime disposizioni di legge in materia è addirittura datata 4 gennaio 1968: si tratta dell'art. 25 della legge 15/68 (“Norme sulla documentazione amministrativa e sulla legalizzazione e autenticazione di firme”) che così recitava: “le pubbliche amministrazioni e i privati hanno facoltà di sostituire, a tutti gli effetti, ai documenti dei propri archivi, alle scritture contabili, alla corrispondenza ed agli altri atti di cui per legge o regolamento è prescritta la conservazione, la corrispondente riproduzione fotografica, anche se costituita da fotogramma negativo”.
Come osservato da A. LISI, “ovviamente l'avvento dell'informativa era lontano, ma già allora moderni sistemi tecnologici aspiravano a sostituire il vecchio cartaceo nella gestione e conservazione dei documenti”[18].
Tralasciando per brevità la puntuale menzione delle innumerevoli disposizioni normative che da allora si sono susseguite, in questa sede sarà sufficiente evidenziare come i processi di dematerializzazione trovano oggi la loro ancora normativa nel CAD e nella deliberazione CNIPA n. 11 del 19 febbraio 2004 (recante le “Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali” e che ha sostituito la precedente deliberazione del 13 dicembre 2001, quando ancora era denominata AIPA). A ciò aggiungasi, per quanto concerne i documenti fiscalmente rilevanti, il già citato D.M.E.F. 23 gennaio 2004.
Prima di entrare in medias res, occorre soffermarsi sulla terminologia propria dei processi di dematerializzazione, e in particolare sui concetti di “memorizzazione”, “archiviazione”, “conservazione”, “riversamento diretto” e “riversamento sostitutivo”.
Per quanto riguarda i termini “memorizzazione”, “archiviazione” e “conservazione” va subito premesso che è importante tenere distinti i tre concetti, giacché è soltanto al termine del processo di conservazione che sarà possibile la distruzione o eliminazione del documento originario.
Con il termine memorizzazione ci si riferisce al processo di trasposizione di documenti analogici o informatici su un qualsiasi supporto idoneo che ne garantisca la leggibilità.
Con il termine archiviazione ci si riferisce al processo di memorizzazione su qualsiasi idoneo supporto di documenti informatici, anche sottoscritti, univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione. In poche parole archiviazione è sinonimo di organizzazione, etichettatura e classificazione documentale.
Infine, con il termine “conservazione”, che si riferisce all’esigenza di mantenere integre nel

tempo le informazioni contenute in un determinato documento si intende al processo che presuppone la memorizzazione su supporti ottici o altri idonei supporti, dei documenti e eventualmente anche delle loro impronte, che termina con l'apposizione della firma digitale e del riferimento temporale sull'insieme dei documenti o su un'evidenza informatica contenente l'impronta o le impronte dei documenti o di insieme di essi da parte del responsabile della conservazione.
Inoltre altre due nozioni di estrema importanza e con le quali è necessario familiarizzare allorquando ci si accosti alla tematica della dematerializzazione sono quelle di “riversamento diretto” e “riversamento sostitutivo”.
Con il primo termine si intende il trasferimento di uno o più documenti portati in conservazione da un supporto di memorizzazione ad un altro, non alterando la loro rappresentazione informatica (classico è l’esempio dei “backup” o copie di sicurezza). Con il secondo, invece, il trasferimento comporta siffatta alterazione (in gergo informatico si usa anche il termine di “migrazione”), per es. per la necessità di un aggiornamento tecnologico dell'archivio informatico, laddove non sia possibile o conveniente mantenere il formato di rappresentazione dei documenti originariamente conservati. La differenza non è da poco giacché se per il riversamento diretto la normativa non prevede particolare formalità, per il riversamento sostitutivo essa prevede l'intervento del c.d. “responsabile della conservazione” che deve assicurare il corretto svolgimento del processo.
Se il riversamento sostitutivo coinvolge poi documenti informatici sottoscritti, allora sarà addirittura necessario l'intervento di un pubblico ufficiale che, apponendo la propria firma digitale, attesterà la conformità di quanto riversato al documento d'origine.
Chiariti questi concetti, si possono ora analizzare più da vicino i processi di conservazione, tenendo distinta, da un lato, la conservazione elettronica dei documenti informatici e, dall'altro, la conservazione elettronica dei documenti analogici (quest’ultima presenta gli aspetti di maggiore interesse consentendo la totale eliminazione degli archivi cartacei).
Per quanto riguarda la prima essa deve essere effettuata mediante memorizzazione dei documenti interessati su supporti ottici o, sebbene non ottici, comunque idonei ai sensi dell'art. 8 della deliberazione n. 11/2004[19] e terminare con l'apposizione sull'insieme dei documenti ovvero su un'evidenza informatica contenente l'impronta o le impronte dei documenti o insiemi di essi, del riferimento temporale e della firma digitale da parte del responsabile della conservazione, figura centrale nei processi di conservazione e disciplinata dall’art. 5 della deliberazione n. 11/2004.
Per quanto riguarda la conservazione sostitutiva dei documenti analogici occorre premettere che vi è una sostanziale differenza a seconda che essa coinvolga documenti analogici originali unici o documenti analogici originali non unici[20].
Solo e soltanto per i primi la chiusura del processo di conservazione necessita della presenza del pubblico ufficiale, chiamato ad apporre la sua firma digitale e il suo riferimento temporale.
Per i secondi, invece, è sufficiente l'intervento del responsabile della conservazione che, dopo aver proceduto alla memorizzazione dell'immagine dei documenti direttamente sui supporti ottici, eventualmente, anche della relativa impronta, appone, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, il riferimento temporale e la propria firma digitale a garanzia della corretta esecuzione del

processo.
Da ultimo l'art. 5 della delibera n. 11/2004 prevede:
ü la possibilità per il responsabile del procedimento di conservazione sostitutiva di delegare a una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate (comma 2);
ü la possibilità di affidare il procedimento di conservazione sostitutiva, in tutto o in parte, in outsourcing, ossia ad altri soggetti, pubblici o privati (comma 3).

Fatturazione elettronica
Il D.Lgs. 20 febbraio 2004, n. 52, che ha dato attuazione alla direttiva 2001/115/CE in materia di semplificazione e armonizzazione delle modalità di fatturazione in materia di IVA, ha apportato importanti modificazioni al d.P.R. 26 ottobre 1972, n. 633. Per quel che in codesta sede interessa è stato modificato l'art. 21, comma 3, del d.P.R. 633/1972, che attualmente dispone come segue:
"L'attestazione della data, l'autenticità dell'origine e l'integrità del contenuto della fattura elettronica sono rispettivamente garantite mediante l'apposizione su ciascuna fattura o sul lotto di fatture del riferimento temporale e della firma elettronica qualificata dell'emittente o mediante sistemi EDI di trasmissione elettronica dei dati che garantiscano i predetti requisiti di autenticità e integrità".
E' intervenuta peraltro in via interpretativa la circolare dell'Agenzia delle Entrate n. 45 del 19 ottobre 2005 che ha ribadito che in caso di emissione di una fattura elettronica, i requisiti di autenticità dell'origine ed integrità del contenuto devono essere garantiti anche mediante l'apposizione della firma elettronica qualificata e lo stesso vale per la trasmissione telematica della fattura elettronica stessa.
A completamento di quanto sopra scritto, si ricordi che l'art. 1, comma 209 della L. 24 dicembre 2007, n. 244 (c.d. "Legge Finanziaria 2008" ha prescritto che l'emissione, la trasmissione, la conservazione e l'archiviazione delle fatture emesse nei rapporti con le amministrazioni dello Stato, anche ad ordinamento autonomo, e con gli enti pubblici nazionali, anche sotto forma di nota, conto, parcella e simili, deve essere effettuata esclusivamente in forma elettronica, con l'osservanza del decreto legislativo 20 febbraio 2004, n. 52, e del C.A.D[21].

Posta elettronica Certificata
Il d.P.R. 11 febbraio 2005, n. 68 contiene il "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3" cui si affianca il D.M. 2 novembre 2005, recante le "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata". Orbene per "Posta Elettronica Certificata" o "PEC" devesi intendere ogni sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici (art. 1, lett. g), del d.P.R. 68/2005). Inoltre ex art. 48 del C.A.D. la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la PEC. La trasmissione del documento informatico per via telematica, effettuata mediante PEC, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

Le ricevute rilasciate dai gestori di PEC[22], la “busta di trasporto”[23] e la “busta di anomalia”[24] sono sottoscritte dai medesimi mediante firma elettronica avanzata (art. 9 del dPR 68/2005).
Inoltre ai sensi dell’art. 4, comma 4, del d.P.R. 68/2005 “Le imprese, nei rapporti tra loro intercorrenti, possono dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione nell'atto di iscrizione al registro delle imprese. Tale dichiarazione obbliga solo il dichiarante e può essere revocata nella stessa forma ”. Ebbene siffatta comunicazione e variazione della disponibilità all'utilizzo della posta elettronica certificata può essere resa mediante l'utilizzo di strumenti informatici, nel qual caso la dichiarazione deve essere sottoscritta con la firma digitale (art. 5 del D.M. 2 novembre 2005).
Da ultimo, l’art. 18, comma 4, del D.M. 2 novembre 2005, stabilisce che l'elenco pubblico dei gestori di posta elettronica certificata è sottoscritto con firma digitale dal CNIPA (ora DigitPA), che lo rende disponibile per via telematica.

Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica
L’art. 65 del CAD prevede che le istanze e le dichiarazioni presentate alle PA per via telematica sono valide, tra l’altro, se sottoscritte mediante la firma digitale, il cui certificato sia rilasciato da un certificatore accreditato[25].

Registro del tirocinio dei dottori commercialisti e registro dei revisori contabili
Il D.Lgs. 23 gennaio 2006, n. 28 (“Attribuzione all'Ordine dei dottori commercialisti e degli esperti contabili di competenze sul registro dei revisori contabili, a norma dell'articolo 5 della legge 24 febbraio 2005, n. 34”) ha precisato quali siano le modalità di tenuta sia del registro del tirocinio per dottori commercialisti sia del registro dei revisori contabili. In particolare l’attenzione va rispettivamente soffermata sugli artt. 3, comma 1, e 5, comma 1, del D.Lgs. 28/2006.
L’art. 3, comma 1, così dispone:
“La domanda per l'iscrizione nel registro del tirocinio di cui all'articolo 7 del decreto del Presidente della Repubblica 6 marzo 1998, n. 99, conforme alle prescrizioni di legge in materia di bollo, è presentata dal tirocinante, anche in forma digitale, al Ministero della giustizia per il tramite del Consiglio nazionale dei dottori commercialisti e degli esperti contabili. Le modalità di presentazione in forma digitale delle domande e dei relativi allegati avviene mediante documento informatico, sottoscritto con firma elettronica qualificata o con firma digitale, formato, registrato e trasmesso in conformità alle disposizioni di cui al decreto legislativo 7 marzo 2005, n. 82, ed alle regole tecniche di cui all'articolo 71 del medesimo decreto”.
Fa eco alla precedente disposizione l’art. 5, comma 1:
“La domanda di iscrizione al registro dei revisori contabili, di cui agli articoli 27 e 28 del decreto del Presidente della Repubblica 6 marzo 1998, n. 99, conforme alle prescrizioni di legge in materia di bollo, è presentata, anche in forma digitale, al Ministero della giustizia per il tramite del Consiglio nazionale dei dottori commercialisti e degli esperti contabili. Le modalità di presentazione in forma digitale delle domande e dei relativi allegati avviene mediante documento informatico, sottoscritto con firma elettronica qualificata o con firma digitale, formato, registrato e trasmesso in conformità alle disposizioni di cui al decreto legislativo 7 marzo 2005,

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

n. 82, ed alle regole tecniche di cui all'articolo 71 del medesimo decreto".

Il nuovo "Codice dei contratti pubblici"
Il D.Lgs. 12 aprile 2006, n. 163 e succ. modif., contenente il "Codice dei contratti pubblici relativi a lavori, servizi e forniture in attuazione delle direttive 2004/17/CE e 2004/18/CE" ha disciplinato in modo organico e unitario la materia della contrattazione pubblica. Talune disposizioni di codesto Codice prevedono esplicitamente la possibilità di servirsi delle nuove tecnologie nelle varie fasi delle procedure di evidenza pubblica. Per es. l'art. 73 del Codice prevede per le imprese che intendano partecipare a un gara la possibilità di presentare la relativa domande di partecipazione anche in formato elettronico, purché il documento che contenga le domanda medesima sia sottoscritto con firma digitale. L'art. 74 del Codice prevede la stessa possibilità per la presentazione delle offerte. L'art. 77 risulta poi particolarmente indicativo in ordine alla possibilità di utilizzare le nuove tecnologie in ogni fase delle procedure e per ogni comunicazione rilevante, in particolare:
ü tutte le comunicazioni e tutti gli scambi di informazioni tra stazioni appaltanti e operatori economici possono avvenire, a scelta delle stazioni appaltanti e a seconda dei casi, mediante posta, mediante fax, per via elettronica o per telefono (comma 1);
ü in virtù dei principi di neutralità tecnologica, di non discriminazione, di concorrenza, di libero mercato e di parità di trattamento, quando le stazioni appaltanti chiedano o acconsentano alle comunicazioni per via elettronica, gli strumenti da utilizzare per comunicare per via elettronica, nonché le relative caratteristiche tecniche, devono essere di carattere non discriminatorio, comunemente disponibili al pubblico e compatibili con i prodotti della tecnologia dell'informazione e della comunicazione generalmente in uso (comma 5, primo alinea);
ü gli scambi di comunicazioni tra amministrazioni aggiudicatrici e operatori economici deve avvenire tramite PEC ai sensi dell'art. 48 del CAD, del d.P.R. 68/2005 e del d.P.R. 445/2000 (comma 5, ultimo alinea);
ü le offerte presentate per via elettronica possono essere effettuate solo utilizzando la firma elettronica digitale come definita e disciplinata dal CAD (v. anche l'art. 74 del Codice).

Infine l'art. 167 del Codice, concernente le norme generali sulla procedura di approvazione dei progetti per infrastrutture di interesse strategico nazionale e per insediamenti produttivi, prevede che il soggetto aggiudicatore, in alternativa all'invio su supporto cartaceo, ha facoltà di provvedere alla trasmissione (alle amministrazioni interessate e agli enti gestori delle reti) del progetto e degli elaborati necessari alla approvazione dello stesso, muniti di firma digitale, su supporto informatico non modificabile.

Misure di sicurezza per i dati genetici
In data 22 febbraio 2007 è stata emanata dal Garante per la protezione dei dati personali l'Autorizzazione generale al trattamento dei dati genetici[26] (in Bollettino del n. 80/febbraio 2007, pag. 0), autorizzazione che ha poi ricevuto ulteriori proroghe e differimenti, stante la validità temporalmente limitata di siffatta autorizzazione. Orbene il Garante ha prescritto che il trasferimento dei dati genetici in formato elettronico sia effettuato tramite PEC previa cifratura delle informazioni trasmesse da realizzarsi con firma digitale e ciò oltre alla adozione delle ccdd.

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

“misure minime di sicurezza” e di altre cautele indicate nell’Autorizzazione medesima.

Dematerializzazione della documentazione clinica in laboratorio e in diagnostica per immagini
Sempre sul piano della c.d. dematerializzazione e della conservazione sostitutiva, particolare rilevanza assume la documentazione clinica, sia per il valore che assume dal punto di vista strettamente sanitario, sia per quello statistico, sia per quello giuridico. E infatti va menzionato anzitutto quanto scritto nella Circolare Ministeriale n. 61 del 19/12/1986: “Le cartelle cliniche, unitamente ai referti vanno conservate illimitatamente poiché rappresentano un atto ufficiale indispensabile a garantire certezza del diritto, oltre a costituire preziosa fonte documentale per le ricerche di carattere storico sanitario. Le radiografie e altra documentazione diagnostica vanno conservate per 20 anni”[27].
Per tal motivo il Ministero della Salute ha ritenuto opportuno, nel Marzo 2007, redigere le “Linee guida per la dematerializzazione della documentazione clinica in laboratorio e in diagnostica per immagini – Normativa e prassi”.
Anzitutto per quel che concerne la “cartella clinica elettronica” si rinvia al “Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)”, adottato il 15 febbraio 2007, alla Raccomandazione della Commissione U.E. del 2 luglio 2008 sull’interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche, nonché al Provvedimento a carattere generale del 5 marzo 2009 (in Bollettino del n. 103/marzo 2009, pag. 0) del Garante per la protezione dei dati personali, recante le “Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario”.
Per quel che invece in questa sede interessa, debbono essere messe in evidenza i seguenti aspetti:
- nella diagnostica per immagini, il “referto informatico” deve essere validato digitalmente dal medico refertante;
- il referto di medicina di laboratorio deve essere sottoscritto digitalmente e la firma digitale può essere apposta con diverse modalità a seconda delle necessità organizzative del laboratorio, ossia: firma di un referto singolo previa visualizzazione e conferma[28]; procedura semiautomatica per firmare un lotto di referti selezionate[29]; procedura totalmente automatica di firma di referti pre-validati o comunque individuati in qualche modo[30]. La firma digitale dei referti di laboratorio identifica la responsabilità del Direttore del Servizio e dei dirigenti che possiedono i requisiti previsti per sottoscrivere i referti.
- quanto al ciclo di vita dei referti, la procedura di consolidamento”, necessaria per collegare l’esistenza del documento firmato ad un istante di tempo certo e dimostrabile, si ottiene verificando con la massima accuratezza la validità del certificato digitale e associando al documento in questione una marca temporale.

Trasferimento di quote di S.R.L.
L'art. 36, comma 1-bis, del D.L. 25 giugno 2008, n. 112 (“Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione Tributaria”), conv. in L. 6 agosto 2008, n. 133, così dispone:
«L’atto di trasferimento di cui al secondo comma dell’articolo 2470 del codice civile può essere sottoscritto con firma digitale, nel rispetto della normativa anche regolamentare concernente la

sottoscrizione dei documenti informatici, ed e` depositato, entro trenta giorni, presso l'ufficio del registro delle imprese nella cui circoscrizione è stabilita la sede sociale, a cura di un intermediario abilitato ai sensi dell'articolo 31, comma 2-quater, della legge 24 novembre 2000, n. 340. In tale caso, l'iscrizione del trasferimento nel libro dei soci ha luogo, su richiesta dell'alienante e dell'acquirente, dietro esibizione del titolo da cui risultino il trasferimento e l'avvenuto deposito, rilasciato dall'intermediario che vi ha provveduto ai sensi del presente comma. Resta salva la disciplina tributaria applicabile agli atti di cui al presente comma».
Pertanto, facendo riferimento al vecchio testo dell'art. 2740 c.c., la disciplina precedentemente in vigore prevedeva la necessità dell'autentica notarile ai fini della opponibilità dell'atto di trasferimento ai terzi e alla società, giacché, senza la prescritta forma, non avrebbe potuto effettuarsi il deposito presso il registro delle imprese e, conseguentemente, non sarebbe stato possibile richiedere la relativa annotazione nel libro soci. Ora invece la necessità dell'autentica è stata superata, laddove l'atto di trasferimento sia sottoscritto con firma digitale. Si è in pratica introdotto un doppio binario in forza del quale l'uso della tecnologia digitale giustificherebbe di per sé il venir meno della garanzia di legalità rappresentata dall'autentica notarile.
In questo modo, tuttavia, si è finito per attribuire alla sottoscrizione digitale (limitatamente all'atto di trasferimento della partecipazione in una s.r.l.) una valore superiore al corrispondente autografo, giacché mentre la sottoscrizione in calce al contratto di cessione continuerà a necessitare dell'autentica notarile, ciò non è più richiesto laddove al medesimo contratto siano associate le firme digitali dell'alienante e dell'acquirente.

Libro unico del lavoro
L'art. 39 del D.L. 112/2008 cit., ha previsto l'istituzione del c.d. "libro unico del lavoro" in luogo del "libro paga" e del "libro matricola". Con successivo decreto del Ministero del Lavoro, della Salute e della Previdenza Sociale 9 luglio 2008 sono state fissate le modalità ed i tempi di tenuta e conservazione dello stesso.
Per quel che in questa sede maggiormente interessa, l'art. 1, comma 1, lettera c), del D.M. 9 luglio 2008, introduce la possibilità di tenere il libro unico su supporti magnetici ovvero con sistemi di elaborazione automatica dei dati che garantiscono la consultabilità, l'inalterabilità e l'integrità dei dati stessi, nonché la sequenzialità cronologica delle operazioni eseguite, il tutto nel rispetto delle regole tecniche del C.A.D.
Come chiarito dalla circolare del Ministero del Lavoro n. 20 del 21 settembre 2008, con riferimento alla modalità di tenuta su supporti magnetici, i documenti informatici che compongono il libro unico del lavoro devono essere statici e non modificabili e devono essere emessi, al fine di garantirne l'attestazione della data, l'autenticità e l'integrità, con l'apposizione del riferimento temporale e della sottoscrizione elettronica.

Libri, repertori, scritture e documentazione richiesti dalla natura e dalla dimensioni delle imprese
Il D.L. 9 novembre 2008, n. 185, recante "Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale" conv. in L. 28 gennaio 2009, n. 2, ha introdotto nel codice civile l'articolo 2215-bis in forza del quale i libri, i repertori, le scritture e la documentazione la cui tenuta è obbligatoria per disposizione di legge o di regolamento o che sono richiesti dalla natura o dalle dimensioni

dell’impresa possono essere formati e tenuti con strumenti informatici.
Di seguito il testo integrale della nuova disposizione codicistica:
«Art. 2215-bis. (Documentazione informatica). - I libri, i repertori, le scritture e la documentazione la cui tenuta è obbligatoria per disposizione di legge o di regolamento o che sono richiesti dalla natura o dalle dimensioni dell'impresa possono essere formati e tenuti con strumenti informatici. Le registrazioni contenute nei documenti di cui al primo comma debbono essere rese consultabili in ogni momento con i mezzi messi a disposizione dal soggetto tenutario e costituiscono informazione primaria e originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla legge. Gli obblighi di numerazione progressiva, vidimazione e gli altri obblighi previsti dalle disposizioni di legge o di regolamento per la tenuta dei libri, repertori e scritture, ivi compreso quello di regolare tenuta dei medesimi, sono assolti, in caso di tenuta con strumenti informatici, mediante apposizione, ogni tre mesi a far data dalla messa in opera, della marcatura temporale e della firma digitale dell'imprenditore, o di altro soggetto dal medesimo delegato, inerenti al documento contenente le registrazioni relative ai tre mesi precedenti. Qualora per tre mesi non siano state eseguite registrazioni, la firma digitale e la marcatura temporale devono essere apposte all'atto di una nuova registrazione, e da tale apposizione decorre il periodo trimestrale di cui al terzo comma. I libri, i repertori e le scritture tenuti con strumenti informatici, secondo quanto previsto dal presente articolo, hanno l'efficacia probatoria di cui agli articoli 2709 e 2710 del codice civile[31]».

Impresa in un giorno e “comunicazione unica”
In data 6 maggio 2009 un decreto del Presidente del Consiglio dei Ministri (in G.U. n. 152 del 3 luglio 2009) ha individuato le regole tecniche per le modalità di presentazione della c.d. “comunicazione unica” e per l'immediato trasferimento dei dati tra le Amministrazioni interessate, in attuazione dell'art. 9, comma 7, del D.L. 31 gennaio 2007, n. 7, recante a sua volta «Misure urgenti per la tutela dei consumatori, la promozione della concorrenza, lo sviluppo di attività economiche, la nascita di nuove imprese, la valorizzazione dell'istruzione tecnico-professionale e la rottamazione di autoveicoli», conv. in L. 2 aprile 2007, n. 40. Orbene la c.d. “comunicazione unica” è un procedimento informatico che unifica i diversi adempimenti richiesti dalla legge per dare vita a un'impresa in grado di consentire l'avvio di nuove attività in un solo giorno. La comunicazione unica d'impresa va presentata all'ufficio del registro delle imprese, secondo il previsto modello (approvato con il decreto ministeriale 2 novembre 2007, pubblicato in G.U. n. 296 del 21 dicembre 2007), da presentarsi in modalità telematica oppure mediante supporto informatico. In quest'ultimo caso, ai sensi dell'art. 9, comma 2, del DPCM cit., “la presentazione della Comunicazione unica, firmata digitalmente, su supporto informatico avviene esclusivamente tramite consegna diretta del supporto”. A fronte della comunicazione e successivamente alle verifiche previste ex lege, sempre che abbiano esito positivo, la comunicazione unica viene protocollata. A seguito della protocollazione, il sistema rilascia la ricevuta quale titolo per l'avvio dell'attività e siffatta ricevuta è un documento informatico firmato digitalmente dal conservatore del registro delle imprese o da un suo delegato, con marcatura temporale del momento della firma (art. 13, comma 2, del D.P.C.M. cit.).

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

Atto pubblico informatico redatto dal notaio
Il D.Lgs. 2 luglio 2010, n. 110 reca le “Disposizioni in materia di atto pubblico informatico redatto dal notaio, a norma dell'articolo 65 della legge 18 giugno 2009, n. 69”. In particolare il D.Lgs. 110/2010 ha apportato importanti modifiche alla L. 89/1913. In particolare:
ü il notaio per l'esercizio delle sue funzioni deve munirsi della firma digitale rilasciata dal Consiglio nazionale del notariato (art. 23-bis della L 89 cit.);
ü l'autenticazione di cui all'art. 2703, comma 2, c.c., è regolata, in caso di utilizzo di modalità informatiche, dall'art. 25 del CAD (art. 47-bis, comma 2, della l. 89 cit.);
ü il notaio nell'atto pubblico e nell'autenticazione delle firme deve attestare anche la validità dei certificati di firma eventualmente utilizzati dalle parti (art. 47-ter, comma 3, della l. 89 cit.);
ü le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto pubblico informatico in presenza del notaio con firma digitale o con firma elettronica, consistente anche nell'acquisizione digitale della sottoscrizione autografa e il notaio appone personalmente la propria firma digitale dopo le parti, l'interprete e i testimoni e in loro presenza (art. 52-bis della l. 89 cit.);
ü si rinvia a successivi decreti (non ancora emanati) per individuare le tipologie di ulteriori firme elettroniche che potranno essere utilizzate per la firma dell'atto pubblico (art. 68-bis della legge 89/1913).

Atto amministrativo informatico
Con il secondo decreto correttivo del CAD, è stato aggiunto, tra gli altri, l’art. 23-ter, che ha introdotto la figura del c.d. documento amministrativo informatico. Il comma 1 del sopra indicato articolo prevede che gli atti formati dalle P.A. con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto duplicazioni e copie per gli usi consentiti dalla legge.
Il comma 3 poi disciplina il valore giuridico delle copie informatiche di documenti formati dalla P.A. in origine su supporto analogico ovvero da essa detenuti: esse ad ogni effetto di legge hanno l’efficacia degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata, pur sempre nel rispetto delle regole tecniche di cui all’art. 71 del CAD. In tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico.
Viceversa, al fine di assicurare la provenienza e la conformità all'originale delle copie analogiche di documenti amministrativi originariamente informatici, è apposto a stampa, sulla base dei criteri definiti con linee guida emanate da DigitPA, un contrassegno generato elettronicamente, formato nel rispetto delle regole tecniche stabilite ai sensi dell'art. 71 del CAD e tale da consentire la verifica automatica della conformità del documento analogico a quello informatico.

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

_____

[1] E' appena il caso di precisare che l'attuale testo dell'art. 491-bis c.p., cui in precedenza si è accennato, è stato recentemente modificato dall'art. 3 della Legge 18 marzo 2008, n. 48, recante la "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno". In particolare, al primo periodo, dopo la parola "privato" sono state inserite le parole "avente efficacia probatoria", mentre il secondo periodo, proprio per esigenze sistematiche e di coerenza giuridica, è stato soppresso. Il Legislatore ha così eliminato l'anomalia dell'esistenza di una duplice definizione di documento informatico giuridicamente rilevante, riducendola alfine a quella attualmente presente nel D.Lgs. n. 82/2005.
E' opportuno però far presente che la giurisprudenza in passato aveva rimarcato il fatto che, in materia di reati contro la fede pubblica, in particolare di delitti di falso (materiale o ideologico) commessi da un pubblico ufficiale, questi poteva attraverso l'utilizzo di uno strumento o supporto informatico formare un documento rappresentativo di atti o di fatti, destinato a dare quella certezza alla cui tutela sono preposte le norme penali. A tal proposito cfr. Cass., Sez. V Pen., sent. 25 marzo 2005, n. 11930, in cui peraltro si affermò anche che "l'archivio informatico di una P.A. dev'essere considerato alla stregua di un registro (costituito da materiale non cartaceo) tenuto da un soggetto pubblico, con la conseguenza che la condotta del p.u. che, nell'esercizio delle sue funzioni e facendo uso dei supporti tecnici della P.A., confezioni un falso atto informatico destinato a rimanere nella memoria dell'elaboratore, integra una falsità in atto pubblico, a seconda dei casi materiale o ideologica, ininfluente peraltro restando la circostanza che non sia stato stampato alcun documento cartaceo". Sull'irrilevanza dell'eventuale inesistenza di un documento cartaceo, cfr. anche Cass., Sez. V Pen., sent. 3 settembre 2001, n. 32812, ove in motivazione può leggersi alquanto esplicitamente che "ciò che conta (…) non è il documento inteso come oggetto cartaceo incorporante una attestazione, ma l'atto, vale a dire la manifestazione di volontà o di conoscenza, suscettibile di produrre effetti giuridici per la P.A.".
[2] Si ricordi che la parola "documento" è etimologicamente ricollegabile al verbo latino "docere", ossia insegnare, far apprendere, far conoscere.
[3] Sulla irrilevanza dell'elemento materiale merita menzione quanto affermato da E. GIANNANTONIO: "la scrittura è un concetto ampio comprendente qualsiasi dichiarazione incorporata in un supporto materiale destinato a durare nel tempo. Non contano né il tipo di alfabeto né il tipo di supporto" ("Manuale di diritto dell'informatica", Padova, 1997, 385).
[4] Il documento "scritto", a sua volta, si distingue in documento scritto sic et simpliciter (carte e registri domestici, telegramma e telex, fax, taglie o tacche di contrassegno) e documento scritto e sottoscritto (atto pubblico e scrittura privata, semplice o autenticata). Su tali concetti applicati all'uso delle nuove tecnologie (documento scritto, sottoscrizione) si tornerà nel prosieguo della trattazione.
[5] Testo consultabile all'URL http://www.cnipa.gov.it/site/_files/LineeGuidaFD_200405181.pdf
[6] A completamento di quanto analizzato sul valore formale e probatorio del documento elettronico non sottoscritto, si ricordi che nella versione del CAD precedente al secondo decreto correttivo, l'art. 20, comma 1-bis, disponeva solo in ordine all'idoneità del documento

informatico a soddisfare il requisito della forma scritta e nulla sul valore probatorio, che però poteva inferirsi dall'art. 23 del CAD, che ha aggiunto infatti nella disposizione dell'art. 2712 c.c. la menzione delle riproduzioni "informatiche" tra quelle che 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. Siffatta impostazione era perfettamente in linea con quanto aveva riconosciuto la giurisprudenza ancor prima del dato normativo.

"I documenti informatici privi di firma digitale (si tenga conto che al tempo dei fatti di causa non esisteva altro tipo di sottoscrizione elettronica validamente riconosciuta nel nostro ordinamento n.d.a) vanno ricondotti tra le riproduzioni fotografiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti o cose, la cui efficacia probatoria è disciplinata dall'articolo 2712 c.c." (CASS. CIV., 6.12.2001, n. 11445, in Rep. Foro It., 2001).

La disposizione di cui all'art. 23 cit., dopo il secondo decreto correttivo, è stata trasposta nell'art. 23-quater del CAD, nel chiaro intento di considerare autonomamente sul piano probatorio documento elettronico non sottoscritto e riproduzione informatica.

[7] Cfr. D.Lgs. 1 dicembre 2009, n. 17720, recante la "Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione", in base al quale il nuovo ente DigitPA subentra al CNIPA anche in tutti i riferimenti normativi.
[8] In siffatto decreto sono state definite le modalità di rilascio della casella di Posta Elettronica Certificata o "PEC" ai cittadini che ne facciano richiesta, in attuazione dei principi di cui all'art. 3-bis della L. 241/1990 e succ. modif. (uso della telematica sia tra le varie P.A. nei rapporti interni, sia soprattutto tra P.A. e cittadini) e all'art. 3 del CAD (diritto di cittadini e imprese all'uso delle tecnologie nelle comunicazioni con le P.A. e con i gestori di pubblici servizi). Tra gli aspetti salienti, viene enunciata la gratuità della stessa qualora la richiesta sia effettuata al Dipartimento per l'innovazione e le tecnologie.
[9] L'art. 35 del CAD stabilisce che i dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:
a) sia riservata;
b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;
c) possa essere sufficientemente protetta dal titolare dall'uso (improprio) da parte di terzi.
In definitiva la generazione della firma deve avvenire, in definitiva, all'interno del dispositivi. Tali dispositivi e procedure devono garantire l'integrità (non modificabilità arbitraria, inalterabilità, non falsificabilità) dei documenti informatici a cui la firma si riferisce. Infine i dispositivi sicuri di firma devono essere dotati di certificazione di sicurezza in base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. E la conformità ai requisiti richiesti è accertata dall'Organismo di certificazione della sicurezza informatica.

valore giuridico delle firme elettroniche nell'ordinamento giuridico comunitario e nazional

Attualmente le regole tecniche sono previste dal D.P.C.M. 30 marzo 2009, recante per l'appunto le "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici". Con particolare riferimento alla firma digitale si sottolinea ancora la Deliberazione CNIPA (ora DigitPA) n. 45 del 21 maggio 2009 sulle "Regole per il riconoscimento e la verifica del documento informatico", che ha previsto standard di sicurezza particolarmente elevati e imposto la sostituzione di tutte le Smart Card con numero di serie che inizia con 1202.

[11] Il Decreto del 2008 ha sostituito il decreto del Ministro della giustizia del 14 ottobre 2004 che regolamentava precedentemente la materia, stante anche quanto disposto dall'art. 61 proprio del Decreto del 2004, secondo il quale «le regole tecnico-operative sono adeguate all'evoluzione scientifica e tecnologica, con cadenza almeno biennale".
[12] L'art. 2 del D.M.G. 17 luglio 2008 prevede una serie di soggetti abilitati al SICI e precisamente:
- soggetti abilitati esterni privati e cioè i difensori delle parti private, gli avvocati iscritti negli elenchi speciali, gli esperti e gli ausiliari del giudice;
- soggetti abilitati esterni pubblici e cioè gli avvocati, i procuratori dello Stato e gli altri dipendenti di amministrazioni statali;
- soggetti abilitati esterni e cioè i soggetti abilitati esterni privati e i soggetti abilitati esterni pubblici;
- soggetti abilitati interni e cioè i magistrati, il personale degli uffici giudiziari e degli UNEP.
[13] Il "gestore centrale" è la struttura tecnico-organizzativa che, nell'ambito del dominio giustizia, fornisce i servizi di accesso al SICI ed i servizi di trasmissione telematica dei documenti informatici processuali fra il SICI ed i soggetti abilitati. Il "gestore locale" invece è un sistema informatico che fornisce i servizi di accesso al singolo ufficio giudiziario o all'UNEP ed i servizi dì trasmissione telematica dei documenti informatici processuali fra il gestore centrale ed il singolo ufficio giudiziario o UNEP. Il gestore centrale è una sorta di "postino" elettronico che riceve gli atti in forma criptata, associa ad essi una marcatura temporale, effettua controlli sulla qualità dell'utente e dei messaggi e li smista. I gestori locali decriptano gli atti, effettuano controlli formali su autenticità e integrità dei documenti e li smistano alle cancellerie competenti per l'archiviazione dei dati in essi contenuti, che avviene con importazione automatica attraverso la verifica di un addetto alla cancelleria.
[14] Ai sensi dell'articolo 1, comma 2, lett. a), del D.M.E.F. cit. si intende per documento statico non modificabile "il documento informatico il cui contenuto risulti non alterabile durante le fasi di accesso e di conservazione, nonché immutabile nel tempo".
[15] Per es. i comandi che permettono l'aggiornamento automatico della data.
[16] Per es. le istruzioni in grado di controllare, in modo non voluto da chi apre il documento, l'aspetto e il contenuto dello stesso.
[17] L'art. 5 cit., comma 1, stabilisce che il soggetto interessato o il responsabile della conservazione, ove designato, al fine di estendere la validità dei documenti informatici deve trasmettere alle competenti Agenzie fiscali, l'impronta dell'archivio informatico oggetto della conservazione, la relativa sottoscrizione elettronica e la marca temporale. Orbene il comma 2

del medesimo articolo prevede che sono le Agenzie fiscali che debbono indicare gli ulteriori dati ed elementi identificativi da comunicare unitamente a quelli precedentemente indicati. Finalmente, a distanza di circa sei anni, siffatta disposizione è stata attuata.
3. Le stesse Agenzie rendono disponibile per via telematica la ricevuta della comunicazione effettuata ed il relativo numero di protocollo.
Articolo

[18] A. LISI, La conservazione digitale dei documenti contabili e fiscali alla luce della circolare 36/E dell'Agenzia delle Entrate: aspetti giuridici e strategici, in AA.VV., Conservazione dei documenti informatici, a cura di A. Lisi, Edizioni Cierre, Roma 2007, pag. 25.
[19] Di seguito il testo integrale dell'art. 8: "1. Tenuto conto dell'evoluzione tecnologica e della disciplina dettata dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è data facoltà alle pubbliche amministrazioni e ai privati, ove non ostino particolari motivazioni, di utilizzare, nei processi di conservazione sostitutiva e di riversamento sostitutivo, un qualsiasi supporto di memorizzazione, anche non ottico, comunque idoneo a garantire la conformità dei documenti agli originali, nel rispetto delle modalità previste dalla presente deliberazione".
[20] Il CAD offre talune definizioni, che possono essere integrate da altre presenti in diverse disposizioni di legge e regolamentari. In particolare:
- per "documento analogico" si intende la "rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti" (art. 1, lett. p-bis, del CAD) ovvero un documento "formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta, le immagini su film, le magnetizzazioni su nastro" (art. 1 del D.M.E.F. 23 gennaio 2004);
- per "documenti originali non unici" si intendono i "documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi" " (art. 1, lett. v, del CAD) (si pensi per es. alle fatture, alle ricevute fiscali, agli scontrini fiscali).
Per esclusione sono "documenti originali unici" quelli per i quali non sia possibile risalire al loro contenuto attraverso altre scritture o documenti. Si possono considerare originali unici, a titolo esemplificativo, i titoli all'ordine di cui agli articoli 2009 e segg. c.c., come l'assegno e la cambiale oppure la "scheda carburante".
[21] La trasmissione delle fatture elettroniche avviene attraverso il c.d. "Sistema di interscambio" e con D.M.E.F. 7 marzo 2008 l'Agenzia delle entrate è stata individuata quale gestore del sistema di interscambio. A tal fine l'Agenzia delle entrate si avvale della SOGEI - Società Generale di Informatica S.p.A., quale apposita struttura dedicata ai servizi strumentali ed alla conduzione tecnica di detto sistema di interscambio
[22] Come chiarito dal D.M. 2 novembre 2005 le ricevute e gli avvisi che debbono essere sottoscritti sono le seguenti:
- ricevuta di accettazione, ossia la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata;
- avviso di non accettazione, ossia l'avviso, sottoscritto con la firma del gestore di posta elettronica certificata del mittente, che viene emesso quando il gestore mittente è impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non è possibile accettare il

messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario;
- ricevuta di presa in carico, ossia la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce;
- ricevuta di avvenuta consegna, ossia la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio e' inserito nella casella di posta elettronica certificata del destinatario.
[23] L'art. 1, lett. a), del d.P.R. 68/2005 definisce la "busta di trasporto" come il "documento informatico che contiene il messaggio di posta elettronica certificata".
[24] Per "busta di anomalia" si intende, ai sensi dell'art. 1, lett. q), del D.M. 2 novembre 2005 la busta nella quale è inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un titolare, per evidenziare al destinatario detta anomalia.
[25] Altri strumenti reputati dal legislatore come validi sono:
- la carta d'identità elettronica (c.d. C.I.E.) o la carta nazionale dei servizi (c.d. C.N.S.);
- strumenti diversi dalla C.I.E. e dalla C.N.S., purché consentano l'individuazione del soggetto che richiede il servizio;
- quando le istanze e le dichiarazioni sono inviate via fax (v. anche l'art. 38, commi 1 e 3, del d.P.R. 445/2000);
- se trasmesse dall'autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche di cui all'art. 71 del CAD e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato.
[26] Si ricordi che ai sensi dell'art. 90, comma 1, del D.Lgs. 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali") il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante sentito il Ministro della salute che acquisisce, a tal fine, il parere del Consiglio superiore di sanità. Per dato genetico devesi intendere il dato che, indipendentemente dalla tipologia, riguarda la costituzione genotipica di un individuo ovvero i caratteri genetici trasmissibili nell'ambito di un gruppo di individui legati da vincoli di parentela.
[27] Si ricordi che "la cartella clinica è un atto pubblico che esplica la funzione di diario dell'intervento medico e dei relativi fatti clinici rilevanti, sicché i fatti devono essere annotati conformemente al loro verificarsi" (Cass. sent. n. 22694/2005) e costituisce "atto pubblico di fede privilegiata con valore probatorio contrastabile solo con querela di falso" (Cass. 27 settembre 1999, n. 10695).

[28] Trattasi di firma singola apposta in contesto interattivo. E' il caso della firma digitale che l'utente appone ad uno specifico referto, per es. in radiologia, redatto in modo manuale o quasi manuale. Poiché l'utente costruisce interattivamente il contenuto del documento, dedicando un certo tempo a questa redazione, si può ipotizzare un controllo visivo diretto su tale contenuto.
[29] In caso di firma semiautomatica di lotti di documenti, l'utente firma un insieme di referti già preparati in precedenza. Si pensi all'ordine di grandezza, tipicamente, delle decine o centinaia

di documenti. L’utente ha a disposizione un ambiente operativo che gli permette di vedere una lista dei documenti che possono essere firmati, con la possibilità di navigare lungo la lista e di aprire individualmente qualsiasi documento per esaminarlo nel contenuto.
[30] Questa modalità, corrispondente all’art. 35, comma 3, del CAD, descrive il caso in cui un sistema di firma venga attivato per processare in modo automatico un flusso di documenti – provenienti da altri sottosistemi – che il titolare della chiave privata (quindi del dispositivo di firma) non ha modo di controllare puntualmente. La procedura deve essere realizzata in modo tale che una fase di avvio informi l’utente sui dettagli operativi della procedura automatica e chieda la sua conferma, che verosimilmente dovrà essere accompagnata dall’inserimento delle credenziali per l’attivazione del dispositivo. Difficilmente un sistema di questo tipo utilizzerà una smart-card, più probabilmente farà uso di dispositivi di tipo HSM, acronimo per “Hardware Security Module” in grado di assicurare una procedura automatica di sottoscrizione, una sorta di sistema di “firma massiva”.
[31] Di conseguenza le scritture contabili informatiche regolarmente tenute possono far prova contro l’imprenditore. Esse possono fare prova anche a favore dell’imprenditore, ma solo nei rapporti tra imprenditori e limitatamente ai rapporti relativi all’esercizio dell’impresa.