GIOVANNI DUNI

LE FIRME ELETTRONICHE NEL DIRITTO VIGENTE (OSSERVAZIONI SULLA NORMATIVA ITALIANA NEL 2006)

1. Forma elettronica[1] e firma elettronica.

Fin dalle prime idee di dare valore giuridico ad un documento in forma elettronica[2] fu ritenuto ovvio che ciò potesse avvenire uni-

* Il presente lavoro costituisce la rielaborazione un primo studio in materia destinato agli scritti in memoria di Maria Teresa Serra, ed. Jovene.

Il sottotitolo sta ad indicare la consapevolezza che gli scritti in materia sono destinati ad avere un valore immediato spesso breve, conservando forse una valenza ai fini di una ricostruzione dell'evoluzione. Poiché nel presente lavoro si operano continui riferimenti alle norme vigenti, le argomentazioni sono esposte in modo semplificato, sul presupposto che il lettore abbia presente il testo normativo. A tal fine le fonti principali sono riportate in appendice.

[1] Il Cons. Stato, nel parere 11995/04, nel § 12.1, ha fatto presente alcune incongruenze tra la terminologia scientifica e quella adoperata nel Codice, facendo l'interessante esempio di « digitale » e « informatico », concetti che nel linguaggio tecnologico hanno le funzioni rispettive di genere e specie, e che invece nel codice sono intese inversamente, la prima come specie della seconda. Sottolinea Cammarata, M., *Firme elettroniche. Problemi normativi del documento informatico*, I libri di Interlex, Trento, 2005, p. 23, che il termine più corretto è « digitale » in quanto fa riferimento alla espressione inglese « digit », cifra, ed ai numeri di base del linguaggio informatico 0 e 1. La firma elettronica sarebbe più opportunamente definibile come « firma informatica ». Motiva l'argomentazione osservando che da un lato l'elettronica riguarda una molteplicità di strumenti, tra i quali la radio, e, d'altro canto, che i dati informatici possono essere registrati su banda magnetica o su supporto ottico, che prescindono dagli elettroni. Tuttavia, poiché il linguaggio comune e legislativo non è basato su questi precisi abbinamenti tra terminologia e concetti, anche in questo lavoro « digitale », « informatico », « dematerializzato » ed « elettronico » saranno adoperati indifferentemente. Del resto, anche sul piano tecnico, la memorizzazione ottica e magnetica entrano in gioco in un sistema che ne prevede comunque, anche per la sola lettura, l'utilizzazione attraverso computers e quindi la loro gestione elettronica. A maggior ragione il mo-

camente se erano possibili delle soluzioni tecniche che, in alternativa alle garanzie del mondo cartaceo, potessero in qualche modo garantire anche il documento in forma elettronica.

Forma elettronica e firma elettronica, a parte la somiglianza verbale dei termini, erano considerate inseparabili. Dematerializzazione[3] (*alias*: forma elettronica; alias: documentazione digitale) e firma elettronica (nella più ampia concezione terminologica) sono due facce della stessa medaglia, nel senso che non vi può essere dematerializzazione di attività giuridica se non vi sono tecniche che assicurino l'attribuibilità del documento, e quindi dell'atto, al suo autore[4].

In pratica, posto che l'espressione « firmare » era comunque un uso traslato dal mondo delle carte di un atto non ripetibile in modo identico sul documento elettronico[5], firma elettronica assumeva solo il significato di garanzia realizzata attraverso sistemi vari nel mondo dell'informatica e della telematica. Ancor più traslata è l'espressione « sottoscrizione elettronica », poiché anche l'apposizione della firma digitale è solo una operazione tecnica che investe un documento preparato nella memoria del computer, senza che vi sia alcun « sotto » o « sopra ».

L'avvento della firma digitale sembrò tuttavia circoscrivere a questa tecnologia il concetto, sia pure traslato, di « firma », in quanto questa tecnologia si incorpora nel documento, a differenza di ogni altro metodo basato sulla mera identificazione dell'operatore al momento dell'accesso, ivi compresi i sistemi biometrici, che il « Codice » ha quasi del tutto ignorato, malgrado siano studiati

---

mento elettronico è fondamentale nell'amministrazione digitale, che per l'aspetto più significativo, è amministrazione telematica, basata cioè sulla trasmissione di dati che non può essere che di tipo elettronico. La connessione della elettronica agli aspetti dinamici della materia è sottolineata da G. CIACCI, *La firma digitale*, Milano, 2005, p. 111.

[2] DUNI, *L'utilizzabilità delle tecniche elettroniche nell'emanazione degli atti e nei procedimenti amministrativi. Spunti per una teoria dell'atto amministrativo emanato nella forma elettronica*, in *Riv. amm.*, 1978, p. 407 ss.

[3] È stato osservato che il documento in forma elettronica non è immateriale, ma di una materialità diversa, impercettibile direttamente dall'uomo; DUNI, *Teleamministrazione* voce dell'*Enciclopedia giuridica*, Roma, 1993, § 2.1; DI BENEDETTO e BELLANO, *I linguaggi del processo*, Milano 2002, p. 134; ORLANDO, *La paternità della scrittura*, Milano 1997, p. 97. Va tuttavia osservato che l'avvento della firma digitale, rendendo trasferibile ovunque il documento, duplicabile in un numero indefinito di originali identici, lo sgancia dai supporti, imponendo una nuova teorizzazione. In linea generale, per l'immaterialità del documento informatico, in quanto sganciato dal supporto, MASUCCI, *Documento informatico e sottoscrizione elettronica*, in *Riv. It. Dir. Pubblico Comunitario*, 2004, 541 e segg.

[4] Correttamente è stato negata rilevanza giuridica ai meri files informatici, come conseguenza della sola definizione *p* del « Codice » e dello stesso art. 15 della L. 59/97, omettendo di completare l'indagine interpretativa sulle norme che disciplinano i requisiti specifici quali condizione di validità: CAMMARATA, M., *Firme elettroniche*, cit, p. 53 ss.

[5] Cfr.: G. CIACCI, *La firma digitale*, cit., p. 111-112, dove in nota riporta le opinioni del mondo notarile, che propongono l'espressione « sigillo »: RAGAZZO e GIAQUINTO, *Il sigillo informatico*, in « Notariato », 1997 e BARRESI, *Aspetti comparatistici del notariato tra Italia ed Inghilterra*, in « Vita notarile », ottobre 1998.

attentamente dai tecnici del campo. Le espressioni terminologiche possono essere neutre, ossia ininfluenti sulle realtà, a condizione che nello scrivere e nel parlare si abbia ben chiaro ciò cui ci si riferisce. Nulla escluderebbe quindi di riservare alla sola firma digitale la terminologia « firma » o « firmare » e lasciare ad ogni altra soluzione una più generica definizione di « garanzia » nelle attività di rilevanza giuridica, ivi compresi i documenti in forma elettronica privi della firma digitale e pur tuttavia accettati come validi dall'ordinamento[6].

Riteniamo tuttavia questa proposta terminologica qui ipotizzata non utile: non tanto per un attaccamento alla impostazione originaria che fu data quando il problema fu posto in assenza della tecnologia della firma digitale, quanto perché, a livello legislativo, sono previste equipollenze di tale rilevanza da porre praticamente le soluzioni alternative sullo stesso piano funzionale giuridico. Quindi, pur nella consapevolezza della superiorità della soluzione firma digitale, alla data odierna è da ritenere che esista un concetto ampio di firma elettronica, nell'ambito del quale rientrano soluzioni di garanzia varie, compresa la più evoluta firma digitale.

È opportuno anche precisare che, partendo dalla firma elettronica, un discorso completo finirebbe con l'abbracciare tutta la materia dell'amministrazione digitale. Il presente lavoro non ha questo obbiettivo e neppure la pretesa di esaurire tutte le problematiche legate alle garanzie dei documenti informatici, né di dare risposte certe, ma solo di avviare uno studio della materia, individuando le possibili strade e gli elementi di cui è necessario tenere conto. Soprattutto è bene chiarire che la futura evoluzione normativa potrebbe condurre a strade completamente diverse. Oggi ci si limita ad interpretare soltanto la direttiva comunitaria 1999/93/CE sulle firme elettroniche (che chiameremo brevemente « direttiva comunitaria ») ed il D. Legisl. 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale, che più oltre chiameremo anche « Codice ») così come modificato dal D. Legisl. 4 aprile 2006, n. 159.

Il primo criterio che il giurista deve considerare è quello di affrontare il problema conoscendo le soluzioni teoricamente possibili dal punto di vista tecnologico, ma procedere poi alla verifica in merito al loro *effettivo recepimento nelle fonti del diritto*.

Anticipando alcuni riscontri, vedremo che le norme prendono in considerazione i documenti informatici da più punti di vista ed in diversi articoli, che non sono tuttavia facilmente coordinabili. Non sarà quindi assolutamente possibile una interpretazione

[6] Osnaghi, A., *Firme elettroniche e documento informatico: il codice richiede ulteriori integrazioni*, in ASTRID, Rassegna n. 30 del 2006 in *www.astrid-online.it*. sostiene che la definizione 1 della direttiva comunitaria e la definizione q del « Codice » non definiscano firme, ma solo metodi di autenticazione, a loro volta diversi dalla identificazione; Cammarata, *Firme elettroniche*, cit., passim e p. 41 e segg.

letterale di ciascuna norma, isolatamente considerata, ma occorrerà tenere conto di due fattori: il sistema normativo complessivo in cui si innestano le varie disposizioni, partendo dalle definizioni contenute negli articoli iniziali delle fonti (interpretazione sistematica) ed il mondo reale delle operazioni giuridiche dematerializzate che le norme emanate intendono disciplinare (ricerca della « intenzione del legislatore »). Va precisato che tra le operazioni che andremo ad identificare nelle norme sulla P.A. digitale non vi sono solo accessi ad informazioni o altre attività[7], ma anche veri e propri invii di documenti o partecipazione telematica alla loro redazione.

Per la direttiva comunitaria 1999/93/CE sulle firme elettroniche la « intenzione del legislatore » è in gran parte esplicitata nei « considerando »[8] che precedono la parte normativa vera e propria. Sia per la direttiva, sia per il « Codice dell'amministrazione digitale » è altresì rilevante la realtà sulla quale il legislatore comunitario e nazionale va ad incidere con le norme. Si vuole cioè repentinamente sconvolgere quanto sta già avvenendo nel mondo dell'informatica e della telematica? Oppure si intende accettare un presente operativo, disciplinandolo e mirando ad una graduale transizione verso soluzioni più garantite?

Nel procedere alla interpretazione sistematica non si è sempre agevolati dalle definizioni contenute negli articoli introduttivi delle fonti di riferimento, che riportiamo in appendice; già altri[9] ha riscontrato che talune definizioni non trovano alcuna rispondenza nella normativa[10]; quasi tutte le definizioni comunque si completano in modo molto incisivo con gli articoli susseguenti del Decreto

---

[7] Tra queste attività di rilevanza giuridica che non implicano la formazione di documenti LUCA DE GRAZIA menziona il prelievo di danaro nei Bancomat: *Firma elettronica non avanzata. Una personale opinione sulla c.d. « firma elettronica debole »*, in *Diritto e diritti*, 2004, http://www.diritto.it/materiali/tecnologie/testi.html.

[8] In relazione alle argomentazioni del presente lavoro, tra i considerando si segnalano:

— i vari riferimenti al commercio elettronico, che sottintendono la necessità di liberalizzazione e semplificazione delle regole di firma;

— la modifica ad opera della Commissione dell'incarico ricevuto nel 1997 (cfr considerando n. 3): avrebbe dovuto predisporre una proposta di direttiva sulle firme digitali, ma predispose invece una direttiva sulle firme elettroniche, con ciò attuando una evoluzione di orientamento verso l'opportunità di accettare più soluzioni e non la sola firma digitale.

[9] Cfr.: gruppo di lavoro di ASTRID sull'e-government, nel documento « il codice delle pubbliche amministrazioni digitali: prime osservazioni », pubblicato su *Astrid Rassegna* n. 1 del 28 gennaio 2005, a p. 4, Url. diretto *http://www.astridonline.it/E-governme/Codice-del/ASTRID-Osservazioni-codice-PA-digita.pdf*. Si trattava in verità di osservazioni sulle bozze iniziali del codice, parzialmente accolte dal legislatore delegato; Consiglio di Stato nel parere 11995/04 del 7 febbraio 2005 sulla versione preliminare del Codice, al § 12.1; anche in questo caso vi è stato un accoglimento solo parziale nella redazione dell'art. 1 definitivo, come fa notare Guido SCORZA, nel commento all'articolo 1 del Codice in G. CASSANO, C. GIURDANELLA (a cura di), *Il codice della pubblica amministrazione digitale*, Milano, 2005, p. 7.

[10] Così per la firma elettronica avanzata, ma non qualificata, nella direttiva comunitaria.

legislativo: non solo con quelli che fanno espresso riferimento ad esse, ma con tutti quelli che disciplinano in concreto le operazioni nelle quali entra comunque in gioco un'attività amministrativa, o comunque giuridica, di rilevanza formale.

Altri autori hanno affrontato il tema, concentrando per lo più l'attenzione sulle connessioni tra i presupposti tecnologici e le definizioni contenute nelle fonti[11]. L'intento che ci si pone nelle presenti pagine è quello di completare il quadro interpretativo alla luce dell'intero sistema delle fonti, ossia tenendo anche presenti, come si è già detto, le norme (diverse dalle definizioni) che disciplinano le attività giuridiche in forma elettronica.

2. Un po' di storia.

L'espressione « firmare elettronicamente » nel campo dell'informatica applicata al diritto si rinviene per la prima volta in un lavoro che lo scrivente ebbe a presentare al quinquennale Convegno internazionale della Corte di Cassazione del 1978, pubblicato poi sulla Riv. Amm. della Rep. Italiana[12].

In quegli anni la firma digitale era ancora ignota ai giuristi in genere ed italiani in particolare; « firmare elettronicamente » significava soltanto garantire che l'intervento in forma elettronica fosse compiuto da chi ne aveva il diritto ed il potere.

Accanto al tesserino magnetico del Bancomat, già allora esistente e funzionante, si suggerivano altre tecniche aggiuntive, volte a potenziare la garanzia che il solo tesserino magnetico non sembrava fornire[13].

---

[11] In sede di commento al D.P.R. 445, cfr; il lavoro di G. Ciacci, *La firma digitale*, cit, e di M. Cammarata, E. Maccarone, *La firma digitale*, Milano, 2003, p. 45 ss.

[12] Duni, *L'utilizzabilità*, cit.

[13] Duni, *L'utilizzabilità*, cit., ove, in assenza di tecnologie di firma digitale si suggeriva: « Come il correntista per le banche, così l'abilitato alla firma per gli atti amministrativi, dovrebbe disporre di un tesserino non falsificabile, per mezzo del quale la macchina deve poter riconoscere chi l'ha manovrata e registrare tale avvenuto riconoscimento. Il tutto si accompagnerebbe ad eventuali altri accorgimenti e garanzie. Sull'ultimo rigo dell'atto dovrebbe apparire: *a*) un simbolo che indica la messa in funzione del controllo dell'autenticità; *b*) qualifica, nome e cognome in chiaro di chi ''firma''; *c*) eventuali altre indicazioni in chiaro per il caso di omonimie; *d*) un simbolo indicante che l'operatore ha battuto sulla tastiera una combinazione di lettere e numeri segreti (codice personale). Questa garanzia ulteriore potrebbe essere eliminata per gli atti meno importanti; *e*) un simbolo attestante che è stato introdotto il tesserino personale; che esso appartiene alla persona di cui alle lettere *b*) e *c*) e che il codice di cui alla lettera *d*) è anch'esso esatto e corrispondente agli altri elementi *b*), *c*) ed *e*). La macchina dovrebbe essere tuttavia predisposta per non memorizzare affatto gli atti per i quali il controllo automatico ora detto dia esito negativo; *f*) il codice di identificazione del terminale. Il terminale deve indicarlo necessariamente ed automaticamente; *g*) data ed ora, parimenti inserite necessariamente ed automaticamente; *h*) simbolo attestante il riscontro, operato dalla macchina, che la persona che ha ''firmato'' era abilitata per quel tipo di atti. Anche a questo proposito va osservato che la macchina potrebbe essere predisposta in modo da non recepire affat-

In realtà il giurista non intendeva interferire con i ruoli dei tecnici: ciò emergeva chiaramente dalla voluta ed assoluta genericità del quinto caposaldo della Teleamministrazione, enunciato nel convegno della Corte di Cassazione del 1993[14], che era formulato nei seguenti termini: « *la firma (elettronica) consiste nella identificazione dell'identità dell'operatore a mezzo di tecniche sofisticate* ». In sostanza il giurista esponeva l'esigenza della garanzia degli atti giuridici e « commissionava » ai tecnici la risoluzione del problema.

Ancor prima di quelle date i tecnici di oltre oceano erano alle prese con i problemi della criptazione e decriptazione dei documenti e dei messaggi, allo scopo di migliorarne le tecniche e le soluzioni. La criptazione è una tecnica di vecchissima data, già usata da Giulio Cesare, ma l'avvento dei computer aveva stimolato nuovi studi di geniali matematici della Stanford University.

Questi matematici erano Withfield Diffie, Martin Hellman: il loro obbiettivo era quello di superare il metodo classico della criptazione simmetrica, che richiede il possesso del medesimo codice da parte del mittente e del destinatario, che aveva il difetto di esaurire la sua validità dopo ogni uso[15], o quanto meno richiedeva un sistema di variazione continua. In ogni caso era destinato a mettere in relazione un mittente con un destinatario preciso o al massimo con una cerchia ristretta. Diffie ed Hellman si posero un duplice obbiettivo: elevare la complessità di criptazione al punto di renderla indecifrabile senza il relativo codice; non « bruciare » il codice ad ogni messaggio: con i vecchi metodi era abbastanza facile impossessarsi o decifrare il cifrario di criptazione, con il duplice risultato non solo di potere leggere i messaggi riservati, ma di poter creare abusivamente un nuovo messaggio spacciandolo come proveniente dal reale titolare della chiave di criptazione; l'obbiettivo era di impedire tutto ciò: neppure il destinatario doveva essere in grado di poter creare un messaggio falso, poiché non gli doveva essere fornita la chiave di criptazione. L'invenzione fu la criptazione asimmetrica: una chiave di criptazione per

---

to gli atti provenienti dalle persone non abilitate specificamente per essi. Per gli atti atipici, invece, l'unico riscontro possibile da parte della macchina è quello di cui alla lettera *e*) ». Ed in successivo scritto del 1993 (DUNI, *La teleamministrazione: una « scommessa » per il futuro del Paese*, relazione al 5° Congresso internazionale della Corte di Cassazione sul tema « Informatica e attività giuridica » Roma, 3-7 maggio 1993, I.P.Z.S. - Libreria dello Stato, 1994, II, p. 381 ss) si aggiungeva: « Sulla memoria della scheda si potrebbero registrare anche tutti gli estremi degli ultimi interventi, per un riscontro incrociato con le risultanze del sistema: eventuali discordanze evidenzierebbero abusive intromissioni nel sistema ». Quest'ultima idea deve ritenersi tuttora valida.

[14] DUNI, *La teleamministrazione: una « scommessa » per il futuro del Paese*, cit.

[15] GARDNER, *Un nuovo tipo di cifrario che richiederebbe milioni di anni per essere decifrato*, in *Le scienze*, 1977, Dicembre, p. 126 ss. (*Le scienze* è la versione italiana di *Scientific American*. L'articolo di Gardner era apparso sul numero di luglio della rivista americana).

cifrare un documento ed una differente per leggerlo. In questo modo la chiave di criptazione poteva essere usata più volte. Il documento decriptato non poteva essere alterato neppure di una virgola, pena la non attribuibilità al mittente. Come spiega Gardner nell'articolo citato nella nota precedente, era anche possibile inviare messaggi creati con la nuova tecnica in modo che potessero essere letti solo da destinatari selezionati[16]. Questi matematici compresero anche che la loro invenzione garantiva l'attribuililtà del documento a colui che lo aveva criptato ed iniziarono a parlare di « firma »[17], pur senza intuire appieno le potenzialità rivoluzionarie che si aprivano in campo giuridico.

Nel 1977 gli studi di Diffie ed Hellman furono ripresi da tre ricercatori, Ron Rivest, Adi Shamir e Leonard Adleman, che perfezionarono e incrementarono l'ottica della funzione di « firma » della crittografia asimmetrica e, dopo un primo lavoro pubblicato internamente al MIT[18], divulgarono al mondo della scienza questo nuovo metodo di firmare i documenti[19], che dai loro cognomi prese il nome acronimo di sistema RSA, che useremo anche noi nel presente lavoro con riferimento alla firma digitale realizzata a mezzo della criptazione asimmetrica.

Si tratta, in effetti, una soluzione tecnologicamente avanzata che, come vedremo più oltre, consente garanzie di autenticità che altri sistemi non sono in grado di offrire. Tuttavia, il mondo giuridico e quello dei tecnici rivelò subito una scarsa comunicazione reciproca, tant'è che la scoperta non solo non si diffuse in Italia, ma anche negli USA migrò con lentezza dal mondo dei matematici a quello dei giuristi. La prima legislazione al mondo che disciplinò l'uso della firma digitale fu l'Utah Digital Signature Act (Utah Code §§ 46-3-101 to 46-3-504 — Enacted by L. 1995, ch. 61)[20], che contiene tutti gli elementi essenziali che l'Italia adottò poi nel D.P.R. 531/97 sulla firma digitale.

---

[16] Aggiungendo alla criptazione con il proprio codice segreto il codice pubblico del destinatario.

[17] DIFFIE, HELLMAN, *New directions in Cryptography*, in *IEEE Transection on Information Theory*, novembre 1976.

[18] RIVEST, SHAMIR, ADLEMAN, *On Digital Signatures and Public-Key Cryptosystems*, *MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212*, gennaio 1979. Ne riferisce Gardner nello scritto citato. La vicenda è raccontata in modo alquanto romanzato anche da: LEVY, *Crypto. I ribelli del codice in difesa della privacy*, trad. di Cicconi e Carlotti, Shake ed., 2000, cap. 3.

[19] La pubblicazione conclusiva ufficiale degli studi dei tre ricercatori Rivest, Shamir ed Adleman è: *A method for obtaining Digital signature and public key cryptosystems*, in « Communications of the Acm », vol. 21 (2), pp. 120-126, febbraio 1978.

[20] La legge dell'Utah fu commentata in una brillante tesi di laurea di Francesca Flora: *Evoluzione della informatica nel sistema di governo degli Stati Uniti d'America*, Cagliari, Facoltà di Scienze Politiche, novembre 1996.

A livello federale si dovette attendere il 1998: US Senate, S. 1594, Digital Signature and Electronic Authentication Law (SEAL) of 1998. — US House of Represenatives, H.R. 3472, Digital Signature and Electronic Authentication Law (SEAL) of 1998.

È chiaro quindi che nel 1978 ed anni successivi per ogni giurista si elaboravano idee parallele agli studi dei tecnici e che ognuno agiva all'insaputa degli altri. D'altronde il nostro legislatore, iniziò a pensare alla forma elettronica solo nel 1993, con quel pessimo articolo 3 del decreto 39, istitutivo dell'AIPA[21]: si era ben lungi dal conoscere la soluzione RSA.

Nel 1997 l'Italia tentò il grande salto con la legge 15 marzo 1997, n. 59, che all'art. 15 autorizzò gli atti giuridici in forma elettronica, rimettendo ad un emanando regolamento « i criteri e le modalità di applicazione », ossia le garanzie di paternità degli atti. Il regolamento fu il D.P.R. 10 novembre 1997, n. 513, le cui prescrizioni sono state sostanzialmente in vigore fino al D.Lgs. 23 gennaio 2002, n. 10, che modificò l'art. 10 del D.P.R. 28 dicembre 2000 n. 445 (T.U.D.A.), che aveva recepito il regolamento senza adeguamenti alla sopravvenuta direttiva comunitaria in materia di « firme elettroniche ». La modifica del 2002 recepì invece (con ritardo) la direttiva 13 dicembre 1999 n. 93 del Parlamento e del Consiglio europeo sulle firme elettroniche.

La direttiva 1999/93/CE sembrò sconvolgere il mondo scientifico italiano che si era occupato dell'autenticità dei documenti informatici. Cosa era successo?

Partendo dalla premessa che « il diritto è una cosa seria » il regolamento 513/1997 aveva sposato in pieno il sistema della firma digitale RSA come unico sistema di firma elettronica ammessa e, poiché la sicurezza non risiedeva solo nella tecnologia, ma anche nel modo di gestire ed erogare gli strumenti, aveva stabilito che potessero gestire il sistema, fornire i dispositivi ed i « certificati » per generare la firma digitale soltanto soggetti forniti di particolari requisiti ed accreditati con iscrizione in un apposito albo presso l'AIPA.

Alle istituzioni europee non piacque l'eccesso di rigore scelto dall'Italia, cui si contrapponevano differenti soluzioni accolte in altri Stati, e si accelerò l'emanazione della suddetta direttiva della fine del 1999. L'Italia fu implicitamente accusata da due punti di vista: rallentare il passaggio alla dematerializzazione del diritto (commercio elettronico e facili interazioni tra P.A. e cittadini) e, attraverso l'inderogabilità dell'accreditamento, ostacolare la concorrenza tra possibili erogatori di certificati per la generazione della firma digitale. La direttiva fu quindi un chiaro invito all'Italia a consentire soluzioni alternative; all'Italia va comunque riconosciuto il merito di essere stata la prima in Europa ad avventurarsi in questo campo assai delicato.

---

[21] Commentato in DUNI, *L'illegittimità diffusa degli appalti di informatica pubblica*, in questa *Rivista*, 1995, p. 35 ss.

3. I GRUPPI DI NORME DALLE QUALI DISCENDE IL SISTEMA GIURIDICO DELLE FIRME ELETTRONICHE.

L'Italia si adeguò con un certo ritardo alla direttiva comunitaria, con il D. Legisl. 10/2002, ma, omettendo per brevità i passaggi intermedi, possiamo oggi fare riferimento al Decreto sulla P.A. digitale che, attraverso vari rinvii alla direttiva comunitaria mostra la chiara volontà di adeguarsi ad essa, pur attraverso definizioni un po' diverse ed un successivo articolato complesso. Nelle definizioni del « Codice » manca la firma elettronica avanzata (definizione n. 2 della direttiva[22]), ma, esaminando le rispettive discipline, osserviamo che i commi 1 ed 1-*bis* dell'art. 20 ed 1 dell'art. 21 attuano l'art. 5 della direttiva, che al primo comma contempla la firma basata su un certificato qualificato, prevedendone il pieno valore legale ed al secondo comma dispone che non debba essere negato aprioristicamente valore alle firme diverse da quella e quindi *anche* alla (pur non menzionata) firma avanzata. Sia la direttiva comunitaria, sia il « Codice », quindi, distinguono la firma basata su certificato qualificato da tutte le altre, accomunate quindi da un generico riconoscimento ai fini giuridici: l'Italia ha scelto di affidare al giudice l'attendibilità in concreto del documento senza firma qualificata ed anzi ne prevede anche (se in concreto attendibile) l'efficacia della forma scritta ad substantiam; la mancata previsione, nel « Codice » della « firma avanzata », non è quindi motivo di contrasto sostanziale poiché la stessa direttiva, negli articoli dispositivi, non fa discendere da questa definizione effetti diversi rispetto alle firme più generiche della definizione n. 1[23].

Come indicato nel primo paragrafo, i criteri adottati dal legislatore nel riconoscere validità alla forma elettronica non possono essere ricercati in un ambito circoscritto di poche norme che, per il

[22] La firma elettronica avanzata, così come descritta nella definizione della direttiva comunitaria, è una RSA. Può essere basata su certificato qualificato o meno. Se basata su certificato qualificato deve produrre i più rilevanti effetti di cui all'art. 5, comma 1 della direttiva medesima.

[23] Secondo OSNAGHI, *op. cit.*, nel D.P.R. 28 dicembre 2000, n. 445 (TUDA), era correttamente recepita la direttiva comunitaria dopo le modifiche introdotte dal D. Legisl. 23 gennaio 2002, n. 10 e dal il D.P.R. 7 aprile 2003, n. 137: era riconosciuta la firma elettronica avanzata (RSA) ed era aggiunta quella qualificata. Oggi, osserva l'Autore, la firma avanzata è immotivatamente soppressa e si pongono dubbi sulla conformità alla direttiva. In effetti, come si legge nel testo delle nostre argomentazioni, il salto dalla firma qualificata a tutte le altre, che devono essere valutate dal giudice (anche le RSA non qualificate), appare eccessivo. Tuttavia non ci sembra che sussista una violazione della direttiva, considerando che anche quest'ultima adotta lo stesso criterio ai fini della rilevanza giuridica: firma qualificata (art. 5, comma 1) e tutte le altre (art. 5, comma 2). Secondo CAMMARATA, *Firme elettroniche*, cit., *passim* e p. 41 e segg., la firma avanzata della direttiva comunitaria è la firma debole: altre, inferiori, non ne esisterebbero o comunque non sarebbero firme. In realtà la stessa espressione « avanzata » lascia intendere l'esistenza di firme « non avanzate », con garanzie inferiori.

titolo o per l'esplicito contenuto, esprimono tale finalità. Forma elettronica nel diritto amministrativo, ed amministrazione digitale sono la stessa cosa e pertanto l'intero complesso del Decreto 82/05 deve essere tenuto presente per individuare i criteri che sono stati accolti per discriminare da una parte i documenti informatici ai quali è riconosciuta rilevanza giuridica, con effetti più o meno rilevanti a seconda dei presupposti e delle caratteristiche[24], e dall'altra ogni altro file informatico giuridicamente irrilevante.

Per altro, i gruppi di norme particolarmente rilevanti ai nostri fini sono:

— le definizioni (art. 1);

— la disciplina che ad esse fa espresso riferimento allo scopo di completarne la disciplina (gli artt. della sezione II del « Codice »);

— la disciplina del documento informatico (artt. 20 e 21; in parte anche il 22 ed il 23);

— la disciplina della trasmissione dei documenti: artt. 45, 47 e 48 (con il rinvio in esso al D.P.R. sulla posta certificata n. 68/2005); art. 76;

— la disciplina dell'accesso ai servizi e delle istanze dei cittadini (artt. 64 e 65).

A nostro avviso il sistema giuridico accetta la forma elettronica garantita in almeno quattro modi diversi; per la precisione: quattro categorie di modi diversi, dato che alcune di queste categorie si articolano in molte variabili[25]:

A) la firma digitale che rispetta le indicazioni delle definizioni che prevedono le garanzie più rigorose (definizione *s*, che richiama la *r*, a sua volta basata sulla *f*). In base a questo complesso di rin-

---

[24] Si veda il primo criterio direttivo della legge di delega (art. 10 della L. 29 luglio 2003, n. 229): « *a*) graduare la rilevanza giuridica e l'efficacia probatoria dei diversi tipi di firma elettronica in relazione al tipo di utilizzo e al grado di sicurezza della firma ».

[25] Tra le varie fattispecie è stata individuata anche quella del documento con « segnatura elettronica », ossia con sola validazione dei dati e senza attribuzione di firma (CAMMARATA, M., *Firme elettroniche*, cit., passim e p. 33 e segg. in particolare). Pur non escludendo a priori che tale ipotesi possa essere concretizzata, non ci sembra di poterla riscontrare né negli studi dei matematici statunitensi che portarono alla firma RSA, né nella normativa vigente. La tesi di Cammarata si basa sulla traduzione della espressione « autentication », nella definizione 1 della direttiva, intesa come « validazione »; questa traduzione, oltre a destare dubbi, non è stata accolta dal nostro legislatore nei testi definitivi delle definizioni *q* e *b* del « Codice » (CAMMARATA scriveva prima del D. legisl. correttivo del « Codice », n. 159 del 2006). Inoltre va ricordato che oggi — a fronte della neutralità tecnologica della direttiva e del « Codice » — le tecniche conosciute convergono verso la firma digitale, che nacque come un « sottoprodotto » di una esigenza di criptazione evoluta: il sistema della doppia chiave attribuisce necessariamente ad uno specifico autore la paternità dell'operazione e del relativo documento; pertanto la validazione dei dati con l'uso della chiave privata determina *anche e necessariamente* l'attribuibilità del documento attraverso la chiave pubblica.

Il concetto di validazione dei dati (con la relativa tecnologia) può tuttavia essere utilizzato nell'ambito della nostra proposta che affida alla P.A. ricevente il compito di rendere immodificabili i messaggi ed i documenti che le pervengono senza firma digitale: su ciò si veda oltre.

vii, confermati dal comma 3 dell'art. 24, *firma digitale in senso giuridico* non è qualunque applicazione della tecnologia RSA, ma solo quella che risponde a tutti i suddetti requisiti. È possibile una sola variabile, aggiuntiva: l'eventuale accreditamento dei gestori del sistema (certificatori), presso il CNIPA, ai sensi dell'art. 29; accreditamento che è rilevante a taluni effetti ed in particolare ai fini della prima delle tre ipotesi di validità delle istanze presentate alle PP.AA., ai sensi dell'art. 65.

B) La firma con tecnologia RSA, ma che non rispetta le regole di cui alla definizione *s* e relativi rinvii. Secondo il « Codice » non è definibile firma digitale, ma firma elettronica, venendo quindi ad essere equiparata alle firme rientranti nella definizione *q*, pur essendo oggettivamente ad un livello tecnologico superiore; questa ipotesi corrisponde alla « firma elettronica avanzata » di cui alla definizione 2 della direttiva comunitaria;

C) la garanzia derivante da una identificazione all'accesso;

D) la garanzia derivante da un mezzo o modalità di trasmissione affidabile.

Va precisato che per i « documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 71 » (art. 34, comma 2, del « Codice »); premessa una certa problematicità del concetto di « rilevanza esclusivamente interna »[26], questa norma potrebbe avere vasta utilizzazione nella formazione progressiva di documenti unitari che necessitano di apporti di più uffici della stessa P.A[27].

A parte l'ipotesi A, in merito alla quale non sorgono problemi[28], l'efficacia giuridica delle firme elettroniche B, C e D non possono essere oggetto di un dibattito astratto, ma vanno riscontrate nel valore giuridico e negli effetti che il diritto fa discendere da queste differenti forme di garanzia.

---

[26] MASUCCI, *Documento informatico*, cit., p. 564, sottolinea che molti atti interni acquistano rilevanza mediata attraverso l'atto finale del procedimento. Da questa giusta osservazione discende, a nostro avviso, la necessità di rivedere la norma e, nelle more, di dare ad essa una interpretazione estensiva, inglobante le attività *intermedie*, che oggi, nel modo cartaceo, si svolgono in modo semplice ed informale.

[27] Sull'atto a formazione progressiva cfr.: G. DUNI, *Lo sportello unico tra innovazione e remore*, relazione ai convegni di Cagliari e Pisa 1999, in « Il nuovo corso dell'amministrazione locale », Edizioni ETS, Pisa, 2001, ed in www.teleamministrazione.it. Lo studio è poi stato sviluppato in G. DUNI, *L'evoluzione del procedimento amministrativo. Dai procedimenti sequenziali al procedimento a stella*, in *Telejus*, 2004, www.telejus.it.

[28] Come è noto, tuttavia, la firma digitale garantisce che il firmatario è in possesso del meccanismo di firma, ma non garantisce che chi lo usa ne è effettivamente il titolare avente diritto. Sul punto: DUNI, SIDDI, GERRA, GIACALONE, SANNA, *Firma digitale o garanzie biometriche?*, in *Riv. Giur. Sarda*, 2001, 293 e segg. Attualmente l'attivazione del meccanismo per la generazione della firma avviene previa digitazione di un PIN; il massimo delle garanzie si otterrebbe condizionando la generazione della firma ad un riconoscimento biometrico.

In questa materia non è opportuno dare risposte definitive, essendo complessa, opinabile ed in continua evoluzione. Si può essere mentalmente più propensi alla rigidità ed irrinunziabilità delle migliori garanzie, oppure propendere verso una facilitazione della dematerializzazione, attraverso una semplificazione ed una pluralità di metodologie.

Per giungere a conclusioni non puramente preconcette o istintive, occorre abbandonare ogni personale propensione e considerare le norme sopra ricordate, tenendo conto che la società in cui viviamo già opera nella realtà telematica con soluzioni che non si servono della tecnologie RSA nel commercio elettronico e nei rapporti telematici che talune amministrazioni hanno già attivato con i cittadini, nei rapporti interni e con altre PP.AA.

Secondo molti studiosi[29] ogni soluzione tecnica che si discosti dalla firma digitale (o dalla teorica firma qualificata) non merita la qualificazione di « firma », dato che il documento prodotto è un file ordinario che chiunque può creare e alterare. Comprendiamo perfettamente queste perplessità, ma non possiamo ignorare che il nostro compito di giuristi non è quello di definire un concetto astratto di « firma elettronica », bensì di riscontrare quale concetto è stato effettivamente accolto dal legislatore. L'approccio sarà quindi privo di preconcetti « ideologici » o tecnologici puri: gli unici preconcetti che potranno incidere nel dare un significato alle parole testuali delle norme, se preconcetti possono essere definiti, sono la realtà operativa effettivamente esistente e la normativa che concretamente disciplina la materia, al di là delle premesse definitore con le quali non sempre si riscontra una chiara concordanza testuale; occorre cioè considerare tutte le norme nelle quali *il codice prevede che si producono documenti in forma elettronica giuridicamente rilevanti prescindendo dalla soluzione RSA*.

In realtà viviamo un periodo di contrasto tra la tendenza a perfezionare le garanzie, puntando alla RSA, e l'esigenza di non bloccare la realtà. Questo contrasto emerge sia nella direttiva europea sia nel nostro « codice » 82/05.

---

[29] Da ultimi: CAMMARATA, M., *Firme elettroniche*, cit: cfr., in particolare, p. 13 e segg.; nella nota 28, pp. 61-62, critica la rilevanza giuridica data alla posta elettronica semplice, in quanto, pur essendo necessari username e password per l'attivazione, si producono testi non garantiti dalla immodificabilità. OSNAGHI, *op. cit.*, in riferimento alla direttiva comunitaria, osserva: « la definizione di *firma elettronica*, nonostante il nome, non consente di considerarla uno *strumento per apporre una firma*, nel significato pratico comunemente attribuito a questo termine, in quanto non permette di ricondurre i dati cui è applicata ad un soggetto generalmente individuabile e di rendere evidenti le successive modifiche ».

4. Le definizioni e gli articoli ad esse strettamente connessi.

Nell'appendice al presente scritto leggiamo nelle fonti una serie di definizioni articolate, non sempre facilmente comprensibili. Particolarmente oscure appaiono le definizioni 1 della direttiva comunitaria e *q* del « Codice »: « l'associazione logica » dei dati[30], in realtà altro non è che un processo a monte del documento; esaminando le soluzioni concretamente adottate dal legislatore, possiamo affermare che le più significative attengono all'identificazione all'accesso: tant'è che il nostro legislatore — con modifica apportata dal Decreto 159/2006 — ha usato più chiaramente l'espressione « identificazione informatica ». Il De Grazia[31] interpreta l'espressione « metodo di autenticazione informatica » di cui al D.P.R. 445/2000, basandosi sulla corrispondente definizione in lingua inglese e conclude che si tratta di accertamento della identità. Aggiunge poi che da tale processo non si determina una associazione diretta tra le « credenziali » di accesso ed il documento informatico. A nostro avviso, la suddetta definizione contiene una contraddizione intrinseca, emersa nella fase del decreto correttivo 159/2006, che ha modificato in modo rilevante la definizione *q* nel decreto 82/05, sostituendo la vecchia espressione « autenticazione » con quella più chiara per la lingua italiana di « identificazione ». La differenza tra le due espressioni, nella lingua italiana, potrebbe essere vista nei termini seguenti: l'identificazione è l'operazione a monte del messaggio o dell'invio; l'autenticazione è l'effetto: *poiché l'inoltro è avvenuto da parte di persona identificata, esso è autentico*.

Nella sua rigidità era certamente più chiaro il D.P.R. 513/97, che accettando come unico sistema quello della firma digitale RSA, ne definiva gli aspetti operativi. Omettiamo definizioni di fonti con data intermedia e riportiamo solo quelle della direttiva comunitaria e del D. Legisl. 82/2005, nella formulazione definitiva del 2006: ad esse faremo riferimento nel presente lavoro.

Fin dalla direttiva 1999/93/CE, si delineò non solo la volontà di consentire più soluzioni nell'ambito delle tecnologie esistenti, ma anche di lasciare spazio a novità che la tecnologia potesse offrire successivamente. Così che la prima definizione dalla direttiva re-

[30] Cammarata, M., *Firme elettroniche*, cit, p. 33-34, ritiene che le suddette definizioni non disciplinino firme (conforme: Osnaghi, cit.), ma solo validazione di dati, per mezzo di tecnologie che li rendano immodificabili, ma non attribuibili ad un determinato soggetto. Conformemente alla soluzione accolta dal decreto correttivo 159/2006, alle esigenze del commercio elettronico ed alla successiva normativa di semplificazione amministrativa, la nostra tesi è che le definizioni de quo contemplino mezzi di identificazione, accettati come sufficienti per la validità delle operazioni, compresa la produzione di documenti, e senza che venga richiesta una immodificabilità degli stessi nel momento della produzione.

[31] De Grazia, *Firma elettronica*, cit.

cita: « 1) ''firma elettronica'', dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione ». Il codice dell'amministrazione digitale è alquanto simile: « *q*) 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 »[32]; il codice prevede anche: « *b*) autenticazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie *anche* al fine di garantire la sicurezza dell'accesso »[33].

Tra le numerose altre definizioni sono rilevanti quelle della carta di identità elettronica e della carta dei servizi, strumenti particolarmente rilevanti nella costruzione normativa del « Codice »: (cfr., *infra*, § 6), nonché quelle attinenti alla firma digitale.

Il sistema definitorio sia della direttiva sia del decreto sulla P.A. digitale si articola in numerose voci attinenti alla firma che si incorpora nel documento, ossia alla categoria di firme che più sopra abbiamo enunciato *sub* A). Gli aspetti del sistema definitorio sono da condividere, in vista di un intento verso la crescita dell'utilizzazione della firma digitale, al di là dello stesso D. Legisl., che in gran parte si accontenta ancora delle altre categorie di firme ed in particolare delle C e D (*retro*: § 3).

L'elenco definitorio non appare ispirato ad un ordine preciso, in quando definisce prima gli strumenti e poi le firme cui gli strumenti servono. Nel Decreto 82/2005 la definizione più ampia di firma del tipo A) è quella della lettera *r*), rispetto alla quale la firma di cui alla successiva lettera *s*), è espressamente definita « un particolare tipo ». Allo stato attuale delle tecnologie non si conoscono firme elettroniche qualificate diverse dalla firma digitale:

---

[32] La parola « autenticazione » già presente nella direttiva e nell'art. 1 del D.P.R. 445/2000 (nel testo modificato dal D.P.R. 137/2003) è stata sostituita per evitare equivoci con l'autenticazione vera e propria ad opera di notai e pubblici ufficiali (possibile e talora necessaria anche in un mondo di attività digitalizzata e pertanto prevista dall'art. 25 del « Codice »); altrove è stata lasciata: occorre leggerla sempre nel significato corretto. Secondo CAMMARATA, *Firme elettroniche*, cit, p. 28 e segg., il termine inglese « autentication » è riferito ai dati — e va tradotto come « validazione » — o alla provenienza e riguarda la identificazione. Tuttavia, nella definizione *b* del « Codice », vi è una assoluta mescolanza di tutti i profili, soprattutto dopo l'inserimento della congiunzione « *anche* » ad opera del decreto correttivo 159.

Ad avviso dello scrivente il testo del D. Legisl. 82/2005 rende ancora più palese che la firma elettronica de quo (c.d. firma elettronica semplice) è solo una identificazione all'accesso, cui segue eventualmente la creazione o la trasmissione di un documento informatico. Sulla normativa del T.U.D.A.: MASUCCI, *Documento informatico e sottoscrizione elettronica*, cit.

[33] La congiunzione « anche » è aggiunta dal decreto correttivo ed appare significativa: oltre al mero accesso, è consentita quindi attività giuridicamente rilevante. La definizione di cui alla lettera *b*) trova quindi conferma nella definizione *q*).

la lettera r appare quindi enunciata solo per dare spazio a future scoperte. Oltre tutto traspare una certa incoerenza tra una apparente libertà di scelte e l'ultima parte della definizione *r*, che richiede per la più generica firma qualificata, il certificato qualificato ed il dispositivo sicuro, concetto questo che riscontriamo solo nell'allegato III della direttiva comunitaria, che le definizioni ignorano, ma che troviamo comunque richiamato solo oltre, nel decreto 82 (art. 35).

Poiché scopo del presente lavoro è solo quello di distinguere le grandi categorie di firme elettroniche, si evita di entrare in tutte le specificazioni tecniche ed organizzative non indispensabili per le considerazioni attinenti alle linee generali della funzionalità.

Le definizioni operano delle differenziazioni delle firme digitali desunte sia dall'art. 1, sia dal restante contesto del decreto e sono basate sulle caratteristiche: 1) del dispositivo; 2) del soggetto che fornisce i « dati per la creazione della firma » ed i « dati per la verifica della firma »[34] e gestisce il sistema (certificatore) e 3) sulle attestazioni che devono emergere dall'uso del dispositivo e dalla sua verifica presso il certificatore (certificato); i confini tra i suddetti gruppi di regole non sono netti ma molti profili della sicurezza si intrecciano nelle suddette caratteristiche.

Le indicazioni del legislatore nazionale si basano sugli allegati della direttiva comunitaria: l'allegato I, relativo al certificato elettronico e l'allegato II, riguardante il certificatore. Gli allegati alla direttiva sono per la verità quattro. L'allegato III (riguardante i dispositivi di firma) è considerato nel decreto 82 all'art. 35, che, completando in un certo senso il sistema definitorio, disciplina la firma sicura, basata sull'allegato suddetto. Non viene mai richiamato formalmente l'allegato IV, che contiene raccomandazioni per la verifica della firma sicura, per lo più o già accolte dal nostro legislatore o comunque da completare a mezzo delle norme tecniche.

5. Gli artt. 20, 21 e 23.

Gli artt. 20 e 21 trattano del documento informatico in senso sostanziale e come mezzo di prova. Da queste disposizioni parrebbe che il documento informatico debba essere un file avente particolari caratteristiche intrinseche, che diano garanzie di « qualità, sicurezza ed immodificabilità ». Quando queste garanzie sono quelle della firma digitale di cui alla lettera *s*) delle definizioni (o della

[34] Le espressioni tra virgolette sono contenute nelle definizioni 4 ed 8 della direttiva comunitaria e corrispondono alla chiave pubblica ed alla chiave privata della criptazione asimmetrica. Non si riscontrano nelle definizioni del decreto 82/2005, ma si rinvengono nel contesto (artt. 28, 29, 30, 32).

teorica *r*), il documento soddisfa i requisiti della forma scritta ai fini sostanziali e probatori. Se queste garanzie sono minori rispetto alle previsioni delle definizioni *s*, *r*, e da esse richiamate, sono liberamente valutabili dal giudice[35]. In linea generale, quindi, il livello non qualificato potrà valere inter partes tra coloro che hanno preventivamente accettato una metodologia diversa (sedicesimo considerando della direttiva comunitaria) oppure sarà liberamente valutabile dal giudice ai sensi dei commi 1-*bis* dell'art. 20 ed 1 dell'art. 21.

Tuttavia la conclusione di cui sopra non è affatto certa. È infatti necessario proseguire con l'analisi delle altre disposizioni del Codice della P.A. digitale, nelle quali si riscontra una maggiore apertura del legislatore verso garanzie diverse dalla RSA. Comunque, anche i suddetti commi degli artt. 20 e 21, nella loro ampiezza e genericità, riguardano anche le firme non RSA: ossia anche quelle garantite solo dalla verifica dell'accesso; quindi le firme digitali non qualificate e le firme garantite dalla mera identificazione all'accesso sono a tali fini perfettamente equiparate, nel senso della libera valutabilità in giudizio.

È per altro da rilevare che tali commi prevedono — tra i criteri di cui il giudice dovrà servirsi — l'immodificabilità. Sappiamo che l'immodificabilità di un documento si può avere o creandolo con la tecnologia RSA, anche non qualificata[36], oppure conservando il documento su supporto WORM[37], ovvero ancora applicando una firma digitale di sistema al momento della ricezione, possibilmente in modo automatizzato (su ciò: infra). La tecnologia RSA fornisce le maggiori garanzie, in quanto il documento nasce di per sé immodificabile, mentre la memorizzazione su supporto immodificabile prevede un intervallo tra la memorizzazione magnetica (HD) o elettronica (RAM; pen drive) ed il trasferimento su disco WORM. Es-

---

[35] Già nel testo unico ora abrogato era prevista questa libera valutazione (pur senza fare riferimento al giudice: art. 10, così come sostituito dal D. legisl. 23 gennaio 2002, n. 10). In sostanza l'Italia, a differenza degli altri Stati europei, non richiede la firma qualificata, per integrare il requisito della forma scritta; sul punto: MASUCCI, *Documento informatico*, cit., p. 566.

[36] CAMMARATA, *Firme elettroniche*, cit., p. 31.

[37] DUNI, *La teleamministrazione: una « scommessa » per il futuro del Paese*, cit.: si veda il nono « caposaldo » della teleamministrazione, che prevede l'utilizzazione di dischi WORM (Write Once Read Many): in sostanza, allo stato delle attuali tecnologie, supporti ottici non riscrivibili. Cfr. deliberazione CNIPA n. 11/2004 del 19 febbraio 2004 (pubblicata in G.U. 9 marzo 2004, n. 57), recante « Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali », che sostituisce la precedente deliberazione del 2001 (n. 42 del 13 febbraio). La delibera è accompagnata dalle note esplicative. Nella delibera non si parla espressamente di dischi WORM, ma genericamente di « impiego della tecnologia laser »; nelle note esplicative invece si dice espressamente che « La deliberazione autorizza l'utilizzazione di un qualsiasi tipo di supporto di memorizzazione che consenta la registrazione mediante la tecnologia laser; quindi, non soltanto dischi ottici WORM e CD-R, ma anche magneto-ottici e DVD ». http://www.cnipa.gov.it/site/_contentfiles/01381700/1381795_Deliberazione%2011_2004rtf.zip.

sendo queste tecnologie in continua evoluzione, si può confidare che si realizzino soluzioni di memorizzazioni dirette, immediate ed immodificabili: un obbiettivo che i giuristi pongono al mondo delle tecnologie. Analogamente sussisterebbe una doppia fase adottando la soluzione della criptazione asimmetrica del file pervenuto.

Allo stato attuale, comunque, occorre risolvere il problema interpretativo se l'immodificabilità data dalla memorizzazione WORM, attualmente possibile, risponde al requisito di cui all'art. 20, comma 1-*bis* e 21, comma 2-*bis* al punto da togliere al giudice ogni necessità di valutazione di idoneità tecnica ed equiparando — in un certo senso — la fattispecie rispettivamente a quelle dei commi 2 dei suddetti articoli. Ad avviso di chi scrive l'intervallo tra fase della memoria elettronica e la memorizzazione WORM impedisce, oggi, una equiparazione *ex lege* (nel senso che si possa prescindere dalla valutazione del giudice) della forma elettronica alla forma scritta (*ad substantiam* o *ad probationem*), in assenza della firma digitale. Tuttavia una buona organizzazione dei sistemi informatici delle organizzazione (ed in particolare delle PP.AA.) nelle attività di trasferimento dei dati su supporti WORM, possibilmente quotidiane, dovrebbe accrescere notevolmente il livello di affidabilità e quindi di valutazione positiva da parte del giudice.

Parimenti adeguate garanzie possono ravvisarsi con il sistema della criptazione a carico della P.A. ricevente, con finalità di validazione di dati; garanzie particolarmente elevate se l'operazione è automatizzata ed immediata e se il tutto viene rispedito al mittente a titolo di ricevuta.

La valutazione complessiva degli artt. 20 e 21 ci induce tuttavia ad equipararli in qualche modo alle definizioni di cui all'art. 1, del quale costituiscono un completamento. Gran parte dell'effettiva disciplina del documento informatico va infatti ricavata dalla lettura di altre disposizione che fanno riferimento a specifiche attività giuridiche.

Altra osservazione che occorre fare è che i suddetti articoli, pur con qualche sfumatura di espressione, adottano gli stessi criteri nel dare valore alla forma elettronica, sia essa *ad substantiam* ovvero *ad probationem*, tenuto anche conto che il rinvio all'art. 2702 c.c., contenuto nell'art. 21, comma 2, è accompagnato dalla regola, aggiuntiva, della non ripudiabilità, salvo prova contraria, che è comunque implicita anche nel comma 2 dell'art. 20. In sostanza il « Codice », attraverso due articoli paralleli, usa un unico sistema di criteri per dare valore alla forma elettronica[38].

[38] Alla luce del T.U.D.A., il De Grazia, L., *Firma*, cit., giungeva per altro ad una sostanziale differenziazione tra le esigenze della forma scritta ad substantiam (necessità della firma digitale) e della semplice rilevanza ad probationem, per la quale appariva sufficiente la « firma debole ». Per quanto oggi il « Codice » contempli la disciplina dei contratti immobiliari solo nel comma 2 dell'art. 20, tuttavia, con nor-

Un cenno alle garanzie delle copie di atti e documenti informatici (art. 23). Dopo una estensione della normativa delle riproduzioni meccaniche alle riproduzioni informatiche (generale onere di eventuale disconoscimento), l'art. 23 prevede le copie su carta di documenti informatici e le copie informatiche di documenti sia cartacei che informatici; le prime sono regolate in modo analogo alla vigente disciplina delle copie cartacee di documenti cartacei[39], mentre per le seconde la asseverazione di conformità deve essere garantita con la firme digitale di chi forma la copia e secondo le emanande norme tecniche.

Un commento appare utile in merito al comma 3. La norma non è del tutto chiara, ma, con interpretazione a contrario rispetto ai commi 4 e 5, che si riferiscono alle copie informatiche di documenti cartacei, deve ritenersi che si riferisca a copie informatiche di documenti informatici; quanto meno si riferisce anche a questi. Anzitutto va osservato che se l'originale è munito di firma RSA la copia non ha bisogno di alcuna asseverazione di conformità, in quanto ogni esemplare riprodotto del documento è identico al primo ed è munito della firma digitale dell'autore; si sostiene invero che gli esemplari identici di documenti muniti di firma RSA siano tutti degli originali[40]. Ed allora il comma 3 si riferisce ai do-

---

ma di rilevanza generale (comma 1bis), riconosce il valore ad substantiam alle firme elettroniche di altro tipo. Né può dirsi che tali firme debbano essere firme RSA con garanzie diverse (minori) rispetto a quelle delle definizioni *s*, *r* ed *f*, poiché proprio nel diritto amministrativo avremo modo di riscontrare il riconoscimento della validità di documenti, già necessariamente cartacei ed ora elettronici, senza firme digitali di alcun tipo.

[39] Cfr.: il 6° caposaldo della teleamministrazione, DUNI, *La teleamministrazione*, cit.

[40] Analizzando l'art. 20 del T.U. 445, A. MASUCCI, *Il documento amministrativo informatico*, in G. ARENA, M. BOMBARDELLI, M.P. GUERRA, A. MASUCCI, *La documentazione amministrativa*, Rimini, 2001, p. 214, afferma che « Sulla base della premessa che il documento informatico con firma digitale abbia una ''autonomia'' completa dal contingente supporto dove è memorizzato e che ci troviamo di fronte a un documento del tutto immateriale, duplicabile e trasmettibile telematicamente senza che esso perda il suo valore giuridico, per il legislatore non ha più senso la distinzione tra originale e copia di un documento informatico ». La questione è affrontata anche da M. CAMMARATA, E. MACCARONE, *La firma digitale sicura*, Milano 2003, p. 96-98, dove peraltro gli autori fanno notare che alcuni documenti cartacei non possono essere resi in forma elettronica perché per essi è determinante l'unicità fisica. Fanno l'esempio della cambiale. ZAGAMI, *Firma digitale e sicurezza giuridica*, Padova, 2000, a p. 200 afferma chiaramente che « non ha più alcun senso una distinzione tra ''originale'' e ''copia'' di un documento informatico, in quanto ogni copia informatica è identica al suo originale se composta dagli stessi *bits*, essendo indipendente dal contingente supporto: al termine ''copia'' è preferibile il termine ''duplicato'' ». Sulla « pluralità di originali » ci si è già espressi in più scritti: G. DUNI, *L'autenticità degli atti in forma elettronica*, in *Rivista giuridica sarda*, 2001, fasc. 1, pag. 295-298, dove si afferma che « La firma digitale segue l'atto ovunque esso vada ed ovunque sia memorizzato, con tale precisione da potere quasi diventare un problema, a causa della non distinguibilità dell'originale dalla copia. Ma forse questa perplessità nasce spontanea in noi che siamo nati e cresciuti in un mondo in cui il documento ha un quid di materiale ed a fatica abbiamo sostituito la materialità cartacea con la materialità della magnetizzazione o della incisione laser dei bit elettronici. Assuefacendoci al concetto di dematerializzazione, il numero e la sede degli esemplari non è più importante. Purché, naturalmente, l'atto sia disponibile nel momento e nella sede in cui serve », e G. DUNI, *L'evoluzione*

cumenti informatici privi di firma RSA, garantiti quindi da una firma elettronica che non si incorpora nel documento: in pratica di documenti in possesso della P.A. prodotti o acquisiti a mezzo di identificazione all'accesso e che dovrebbero essere conservati su supporti WORM. Il comma 3 impone, per la copia di questi documenti, garanzie maggiori di quelle richieste per l'originale. La norma, malgrado l'apparenza, non rappresenta una anomalia: *il documento privo di firma digitale non può circolare liberamente nella società*, poiché si tratterebbe di un file privo di ogni garanzia, a cominciare dalla immodificabilità; *esso ha valore solo e fintanto che viene custodito da un soggetto garante della sua custodia*[41]. È quindi perfettamente logico e coerente che, per farlo circolare liberamente al di fuori del sistema della P.A., sulla copia venga apposta la firma digitale del funzionario incaricato.

In aggiunta alle considerazioni di cui sopra, abbastanza tradizionali dato che l'idea della soluzione WORM risale al 1993, si è già più sopra accennato ad un'altra proposta: ogni P.A. dovrebbe essere munita di firma digitale di sistema[42], che in modo automatico si applica ai messaggi dei cittadini, garantendo la conservazione immodificabile del documento; il tutto potrebbe essere inviato al cittadino sotto forma di ricevuta, secondo quanto si esporrà nel § seguente.

6. Gli artt. 64 e 65.

Per chi ritiene che i documenti informatici giuridicamente validi siano solo quelli muniti di firma RSA, la coerenza funzionale del

del procedimento amministrativo. Dai procedimenti sequenziali al procedimento a stella, in *Telejus*, 2004, www.telejus.it, dove la problematica è trattata con ampiezza.

[41] Con riferimento specifico al documento siglato con chiave biometria, si affermava (G. Duni, *L'autenticità degli atti in forma elettronica*, in *Rivista giuridica sarda*, 2001, fasc. 1, pag. 295-298) che « Una volta emanato l'atto, esso deve essere custodito in modo fisicamente protetto dall'amministrazione che lo detiene, la quale deve proteggere sia i locali dove è conservata la memoria di massa, sia il sistema informatico da ingressi abusivi di hakers ». Ed in precedenza (G. Duni, *La teleamministrazione come terza fase dell'informatica amministrativa. Dalla* « informazione automatica » *sulle procedure burocratiche al procedimento in forma elettronica*, in G. Duni, a cura di, *Dall'informatica amministrativa alla teleamministrazione*, Roma, 1992, p. 34): « Deve poi essere sempre e facilmente possibile un controllo da parte del sistema e del funzionario stesso che altri non abbia fraudolentemente redatto atti attribuiti a lui. Tale controllo potrebbe addirittura essere quotidiano ed automatico, con elevazione del livello di garanzia del sistema mai raggiunto "nell'era delle carte".

Gli archivi devono essere costituiti da memorie di massa duplicate e collocate contemporaneamente in almeno due posti distinti e difesi. Deve essere preferito il sistema di archiviazione "WORM", che non consente di alterare quanto memorizzato. Nel caso che si scopra un errore in un atto memorizzato, deve essere effettuata una procedura palese di correzione, che mantenga cioè in memoria il testo errato e quello corretto ».

[42] Trattadosi di intervento automatico non attribuibile ad un individuo particolare, questa particolare utilizzazione della tecnica RSA potrebbe essere un caso di « validazione di dati » senza firma, di cui parla Cammarata, *Firme elettroniche*, cit.

sistema comincia a vacillare nell'art. 64 e più decisamente nel 65 del « Codice »; conseguentemente anche il rigore terminologico in merito alla « firma » di un documento informatico necessita di una « correzione di rotta ». L'art. 64 disciplina l'accesso ai pubblici servizi ed in molti casi sarà necessaria una operazione di rilevanza giuridica, quale una prenotazione o una vera e propria istanza. Ma per l'istanza abbiamo l'art. 65, più specifico.

Come si evince da tali disposizioni, il legislatore prende atto della situazione attuale della mancata diffusione delle firme digitali e, pur menzionandole al primo posto nel comma 1 dell'art. 65, accetta: *a*) fino al 31 dicembre 2007 operazioni e documenti garantiti anche soltanto da password e PIN; *b*) a tempo indeterminato operazioni e documenti garantiti da un previo accesso tramite carte di servizi e carte di identità elettroniche. Tutti strumenti che lasciano in mano alla P.A. o all'erogatore di servizi tracce di attività e veri e propri documenti informatici costituenti files che nulla hanno di incorporato assimilabile alla firma digitale e che non sono tecnicamente difesi da immodificabilità, salva la custodia su supporti non modificabili ovvero la criptazione ad opera della stessa P.A., di cui si è più sopra detto.

A nostro avviso queste scelte, almeno allo stato attuale della diffusione delle tecnologie, sono in linea di massima da condividere perché ogni altra più rigorosa scelta avrebbe infatti paralizzato un mondo telematico esistente ed ancora in formazione.

Va anche sottolineato che le « Norme tecniche in materia di formazione e conservazione di documenti... », deliberazione AIPA 23 novembre 2000, ancorché emesse sulla base del rigoroso D.P.R. 513/97, disciplinavano documenti informatici muniti di firma digitale « quando prescritta », ammettendo quindi l'esistenza di documenti informatici giuridicamente rilevanti e senza firma digitale (art. 2, comma 1, lett. *c*).

Non è fondata l'obbiezione che le istanze telematiche di cui all'art. 65 siano sostitutive di istanze per le quali non è prescritta la forma scritta: ciò è vero in molti casi, ma non sempre[43]; inoltre va sottolineato che la sostituzione dell'oralità (garantita dalla presenza fisica o quanto meno dalla voce[44]) con l'alternativa dello scritto non obbligatorio, nel mondo cartaceo deve rispettare comunque le regole della validità e dell'attribuibilità degli scritti.

Questo ampio spazio di documenti informatici senza firma digitale sono accettati dalle PP.AA. come autentici, perché trasmessi previa identificazione. Va sottolineato — per questa e per ogni altra ipotesi di tecniche di identificazione-autenticazione on line —

[43] Basti pensare a tutti i casi in cui l'istanza va presentata in bollo; potrà anch'essa diventare telematica, ma dovrà rispettare il comma 5 dell'art. 21 del « Codice ».

[44] Sono noti, per altro, gli incovenienti derivanti dai contratti redatti per telefono attraverso i « call centers ».

che il ricevente, se la tecnica è adeguata, è sufficientemente garantito, poiché il documento sarà da lui stesso custodito. Il mittente, viceversa, deve necessariamente affidarsi alla buona fede del destinatario; per attenuare questo disequilibrio tra le parti sarebbe auspicabile la trasmissione automatizzata di un messaggio di avvenuta ricezione da parte della P.A. destinataria[45], con gli estremi del protocollo informatizzato: questo messaggio potrebbe essere contestato dalla P.A. ed in effetti potrebbe essere costruito artificiosamente da chi intende avvalersene come prova; tuttavia una esatta enunciazione degli estremi di protocollo dovrebbe costituire una sufficiente prova dell'avvenuta trasmissione di *un* messaggio, ancorché non ne sia provato il contenuto.

Se il messaggio di ricevuta fosse munito di firma digitale e riproducesse anche il testo del messaggio del cittadino, la garanzia reciproca sarebbe massima: avremmo in tal modo semplificato le attività del cittadino, esentandolo dal munirsi della firma digitale, ma, poiché la P.A. non ha le stesse difficoltà, certifica essa stessa, con propria firma digitale, quanto il cittadino le trasmette in modo semplificato.

7. Le garanzie nella trasmissione dei documenti: gli artt. 45, 47, 48 e 76.

L'art. 45 (comma 1: « uso di qualsiasi mezzo telematico o informatico, ivi compreso il fax ») contiene una disciplina di una liberalità tale da suscitare qualche timore anche nelle persone più disponibili alla semplificazione. Si tratta infatti di metodologie che di per sé non garantiscono la provenienza. L'intestazione del fax, ad esempio, può essere creata e modificata a piacimento del mittente e chiunque potrebbe creare, anche provvisoriamente, una intestazione di fax e fare apparire un documento come proveniente da altro ignaro cittadino[46]. Il secondo comma attiene alla posta elettronica non certificata (argomentazione a contrario, dato che la posta certificata è prevista dall'art. 48 e relativo regolamento); il comma, facendo riferimento alla disponibilità del documento nella casella del destinatario, tende ad una certa equiparazione alle regole della posta certificata, pur con strumenti del tutto insicuri. Tutte le sicurezze di cui all'art. 45, a nostro avviso vanno ricer-

[45] Nel commercio elettronico ed in molte attività telematiche in Internet l'invio di siffatte ricevute è oggi ordinaria realtà.

[46] Più prudentemente, l'art. 6 della legge 30 dicembre 1991, n. 412, disponeva: « 2. Salvo che per gli atti aventi valore normativo, le comunicazioni tra amministrazioni pubbliche, enti pubblici, regioni ed enti locali che avvengano via telefax sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza. Qualora dalle comunicazioni possano nascere diritti, doveri, legittime aspettative di terzi, prima dell'atto finale del procedimento dovrà essere acquisito agli atti l'originale della comunicazione ».

cate solo nell'affidabilità nel caso concreto, con il buon senso delle parti coinvolte e con eventuali riscontri paralleli. Tutto comunque è lontano anni luce dalle garanzie della firma digitale.

Potrebbe obbiettarsi che la disciplina della trasmissione dei documenti sia cosa diversa dalla valenza giuridica degli stessi, ossia della loro attribuibilità (firma elettronica). Ossia: il fatto che un mezzo di trasmissione sia accettato dall'ordinamento non significa che anche quanto trasmesso sia parimenti accettato come valido. L'obbiezione è intrinsecamente logica; tuttavia dalla lettura della norma traspare chiaro l'intento di semplificazione e quindi dell'accettazione sia del mezzo che del documento, tenuto anche conto dell'obbligo per le PP.AA. di istituire sia una casella di posta certificata, sia una di posta elettronica ordinaria. Unica limitazione che ci sentiamo di proporre è che la trasmissione di documenti di testo privi di firma qualificata o almeno RSA (« avanzata » nella terminologia della direttiva CE) è efficace, quanto al documento « file informatico », se trattasi di documento inviato come proprio del mittente stesso, a cominciare dallo stesso messaggio e-mail; il tutto poi soggetto a valutazione del giudice sulla provenienza in concreto e sulle attribuibilità degli stessi, ai sensi degli artt. 20, 21 e 23.

Altra limitazione alle possibilità previste dall'art. 45 è la proposizione delle formali istanze, la cui disciplina è prevista in modo specifico dall'art. 65, che, in assenza di firma digitale, prevede appositi sistemi di individuazione, ancorché rimessi alla scelta della singola P.A. fino al 31 dicembre 2007 e, successivamente, a mezzo della carta di identità elettronica o della carta dei servizi.

Più articolato è comunque l'art. 47, relativo alla trasmissione tra le PP.AA., nel cui comma n. 2 si trovano parificati, quanto agli effetti, sicurezze attinenti al documento, al mezzo di trasmissione ed alla gestione protocollare della P.A. Ciò conferma, anche ai fini dell'interpretazione dell'art. 45, che il legislatore è orientato verso l'equipollenza di qualunque tecnica che dia sicurezza alle attività giuridiche telematiche ed ai relativi documenti. A parte i rinvii alle regole tecniche di sicurezza (art. 76), si evince dai suddetti articoli che un documento è validamente spedito anche se privo di firma digitale, purché sia dotato di protocollo informatizzato, ovvero sia inviato attraverso posta elettronica certificata. Altra ipotesi, potenzialmente ancora più ampia nella sua genericità, è che sia « comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche ... ».

A parte l'indeterminatezza attuale (in attesa di norme tecniche[47]) di questa ipotesi di carattere generale, occorre prendere

[47] Il « Regolamento per la disciplina del procedimento amministrativo e dell'amministrazione digitale » della Provincia di Bologna (deliberazione del Consiglio

atto che gli artt. 47 e 48, in sostanza, attribuiscono al documento informatico trasmesso valore giuridico « anche ai fini del procedimento amministrativo » (47 comma 1) per il solo fatto che taluni meccanismi ne garantiscono la provenienza[48]. In sostanza, nell'ambito dell'attività interna della P.A. sono l'equivalente dell'uso della carte elettroniche da parte di cittadini che si pongono in relazione telematica con le amministrazioni (artt. 64 e 65).

8. La contestabilità in giudizio dei documenti informatici.

È stato già rilevato[49] che il legislatore ha lasciato un enorme spazio alla valutazione da parte del giudice dell'affidabilità in con-

provinciale n. 6 del 15.02.2006 entra in vigore il 01/04/2006), all'articolo 6, riguardo alla trasmissione tra amministrazioni, dispone che « I documenti informatici della Provincia, validamente formati ai sensi dell'articolo 5 del presente regolamento e delle regole previste dal D.Lgs. del 7 marzo 2005 n. 82 e successive modificazioni, sono trasmessi ad altra pubblica amministrazione in modo che il ricevente possa verificarne la provenienza. A questi fini è di norma utilizzata la posta elettronica certificata, salvo utilizzo del sistema di protocollo informatico interoperabile con l'amministrazione ricevente ». Il regolamento è all'Url http://www.provincia.bologna.it/provbologna/allegati/pagine/749/Reg.%20procedimento%20amm..doc.

[48] È stato sottolineato che la posta certificata garantisce la trasmissione di messaggi e documenti allegati, ma non la paternità (firma elettronica) dei documenti stessi. Da ultima: C. Bernardi, *commento all'articolo 48 del Decreto legislativo 7 marzo 2005, n. 82*, in G. Cassano, C. Giurdanella (a cura di), *Il codice della pubblica amministrazione digitale*, Milano, 2005, p. 470. Ma quasi tutti gli autori lo danno per scontato. Il problema ovviamente esisteva già nel regime cartaceo con riferimento all'istituto della notificazione. Osservava G. Landi, *Notificazione, diritto pubblico* voce dell'*Enciclopedia giuridica*, XXI, p. 1, che « La notificazione non è un elemento dell'atto o provvedimento notificato, bensì un atto esterno e diverso, i cui vizi eventuali non hanno influenza alcuna sulla validità del primo ». La tesi è basata su una indiscutibile realtà tecnica, tuttavia bisogna prendere atto che il legislatore, seguendo la strada della semplificazione, nell'art. 47 accetta la posta certificata come sistema di trasmissione che rende validi i documenti nell'ambito del procedimento amministrativo, ancorché privi della firma digitale, che è giuridicamente un'alternativa alla posta certificata e non già una caratteristica che deve coesistere.

[49] A. Graziosi, *La nuova efficacia probatoria del documento informatico*, in *Riv. trim. di dir. e proc. civ.*, 2003, p. 64, ove afferma con riferimento al 2° comma dell'art. 10 del dpr 445 del 2000 (come novellato dopo la direttiva CE): « La valutazione dell'efficacia probatoria di documenti informatici sottoscritti o formati con uno di questi eterogenei di firma elettronica è rimessa, come qualsiasi altra prova civile (art. 16 c.p.c.), al prudente apprezzamento del giudice. Mi pare che il principale significato pratico e sistematico di questa disposizione stia nell'aver definitivamente legalizzato l'uso di questo tipo di prove, le quali, quindi, d'ora innanzi, dovranno considerarsi inserite a pieno titolo nel catalogo delle prove tipiche. E così, ad esempio, non si potrà più dubitare che una transazione commerciale conclusa con una carta di credito o con un bancomat sia provabile esibendo al giudice la traccia elettronica e/o cartacea lasciata dall'uso di tali strumenti. Fermo, ovviamente, il potere del giudice di valutare la loro attendibilità nel singolo caso concreto ». A. Masucci, *Il documento informatico*, in *Rivista di diritto civile*, 2004, p. 772, afferma che, con riferimento all'ampio potere di valutazione dato dalla legge italiana al giudice (anche lui fa riferimento al primo comma dell'art. 10 del 445): « Si tratta di un potere di valutazione eccessivamente discrezionale. Più ristretto è, infatti, il margine di valutazione riconosciuto al giudice nel diritto francese. Nel *Code Civil* sono, infatti, individuati per legge i *criteri* che dovranno orientare l'apprezzamento del giudice in ordine al riconoscimento del valore probatorio del documento. Nell'art. 1316-1 del *Code Civil* è

creto del documento informatico, ai fini sostanziali e probatori. In effetti, si nota una contrapposizione tra il comma 2 dell'art. 20, ed il comma 2-*bis*, nonché, analoga, tra i commi 1 e 2 dell'art. 21. Si passa infatti dalla assoluta incontestabilità del documento informatico munito di firma digitale qualificata (definizioni *s*, *r* ed *f*) ad un campo vastissimo, nel quale esiste solo il confine inferiore del documento inaffidabile e quindi giuridicamente irrilevante.

Lasciare tanto spazio al giudice non è mai un indice di buona legislazione: il cittadino, infatti, non è in grado di conoscere a priori chi è in torto e chi ha ragione: per togliere ogni dubbio deve entrare in contenzioso, con aggravio proprio e per la generalità. Inoltre, proprio in questo campo ancora poco studiato, l'autonoma valutazione di ciascun giudice porterà a pronunzie discordanti, che accresceranno la confusione per anni, fino a quando la Corte di Cassazione ed il Consiglio di Stato non avranno definito una giurisprudenza chiara nel creare dei criteri che non troviamo espressi negli artt. 20 e 21.

Questo ampio spazio indeterminato è giustificabile solo alla luce della difficile fase che si sta attraversando nel mettere a punto la « rivoluzione » tra il diritto cartaceo e quello digitale. Una riflessione sulle diverse fattispecie che si riscontrano tra la firma digitale qualificata ed un documento privo di ogni garanzia, dovrebbe portare a graduare diversamente, per categorie, gli effetti giuridici. Le categorie potrebbero essere basate sui differenti apparati di garanzie nella conservazione dei documenti; potrebbe altresì essere previsto un qualche valore aggiuntivo ai documenti muniti di firma RSA non qualificata (firma « avanzata » nella direttiva CE)[50], attualmente equiparati ai documenti privi di firma digitale e garantiti solo dalla identificazione all'accesso o dal mezzo di trasmissione sicuro.

Attualmente occorre chiarire l'apparente contrasto esistente tra il rigore delle definizioni e degli artt. 20 e 21 da una parte e le norme commentate nei §§ 6 e 7 del presente lavoro, che potremmo chiamare di « semplificazione amministrativa » (artt. 64, 65, 45,

previsto che l'ammissibilità del documento elettronico come mezzo di prova è subordinato alle condizioni che *a*) possa essere debitamente identificata la persona dalla quale il documento promana; *b*) il documento sia creato e conservato in condizioni che ne garantiscano l'identità ». Con riferimento espresso al « Codice » cfr. G. Cammarota, *Commento alla Sez. I del Capo II del decreto legislativo 7 marzo 2005, n. 82*, in E. Carloni (a cura di), *Codice dell'amministrazione digitale*, Rimini, 2005, p. 184; G. Scorza, *Commento all'art. 21 del decreto legislativo 7 marzo 2005, n. 82*, in G. Cassano, C. Giurdanella, *Il codice della pubblica amministrazione digitale*, Milano, 2005, p. 190. Tratta la questione in modo più problematico M. Orlandi, *Il falso digitale*, Milano, 2003, p. 27.

[50] Secondo Osnaghi, *op. cit.*, le sole firme elettroniche ammissibili dovrebbero essere RSA: « avanzate », secondo la definizione della direttiva o qualificate, che corrispondono alle definizioni più rigorose. La valutazione del giudice dovrebbe riguardare quindi le ipotesi di firme RSA atipiche, ossia non basate su certificati qualificati, con esclusione di altri documenti. Occorre tuttavia prendere atto che il legislatore non ha seguito questa teoria rigorosa.

47, 48 e 76). A nostro avviso occorre distinguere la validità giuridica, indiscussamente riconosciuta dai vari articoli commentati nei citati §§, dalla possibilità della contestazione dell'autenticità, non alterazione e datazione del documento. Del resto in vari commi si condiziona la validità alla verifica della provenienza: verifica di pertinenza delle parti, ma sempre contestabile in giudizio. Il problema è di notevole importanza teorica e pratica: in linea di principio il documento informatico nelle fattispecie commentate nei §§ suddetti è valido, perché così espressamente previsto; tuttavia è sempre possibile contestare il documento, eventualmente prodotto in giudizio da una controparte, contestandone la provenienza, la conformità, l'integrità, la datazione. Comunque opererà una sorta di presunzione abbastanza consistente perché legata a previsioni legislative, di autenticità e di non avvenuta alterazione, nei rapporti con le PP.AA, soprattutto se si riscontreranno opportune tecniche di custodia dei fascicoli informatici, in particolare su dischi WORM, ovvero se la P.A. ha istituito un sistema automatizzato di firma digitale sui documenti in arrivo, con eventuale reinvio al mittente a titolo di ricevuta.

Osserviamo inoltre che la garanzia di una firma RSA, senza certificato qualificato, non trova particolare considerazione nel « codice ». Se applicata ad un documento trasmesso ai sensi del su citato gruppo di articoli (64, 65, 45, 47, 48 e 76), sembrerebbe che non aggiunga nulla dal punto di vista giuridico; in verità una firma RSA darà consistenza all'attendibilità del documento, ma solo ai fini della libera valutazione da parte del giudice, prevista negli artt. 20 e 21.

Si ricade quindi, in sostanza, nelle previsioni degli artt. 20 e 21 del « Codice », che affidano al giudice la risoluzione di siffatti problemi. Ad avviso di chi scrive, mentre nel caso di rapporti tra privati la contestazione del documento avrà spesso ampie prospettive di successo, nei rapporti con PP.AA. la verifica della efficienza dell'organizzazione informatica, accompagnata da tempestive memorizzazioni WORM, dovrebbe fare propendere i giudizi in favore del riconoscimento dell'esistenza e quindi della validità del documento stesso. È da sperare comunque che le previsioni contenute negli articoli esaminati nei §§ 6 e 7 possano consentire una operatività fisiologica di ampia portata e che errori, o, peggio, furbizie, siano eventi molto rari, ancorché possibili e quindi da prevedere.

A completamento del discorso sulle possibili contestazioni in giudizio, occorre osservare che il rinvio all'art. 2702 del Codice Civile, contenuto nel comma 2 dell'art. 21 poteva essere evitato con una autonoma formulazione del comma stesso. Infatti il comma 2 dice quasi il contrario del 2702 c.c., poiché quest'ultimo è basato sul riconoscimento della firma autografa, laddove il comma 2 dell'art. 21, al contrario, presume l'autenticità (ricondu-

cibilità) della firma digitale, addossando la prova contraria al titolare del dispositivo[51].

9. Considerazioni conclusive: firme digitali; altre firme RSA; identificazione all'accesso telematico e trasmissioni sicure: molte soluzioni in un sistema in evoluzione.

Come già detto, nel 2002 il legislatore nazionale, al fine di adeguarsi alla direttiva comunitaria 1999/93/CE ha abbandonato la rigida impostazione del D.P.R. 513/1997, che aveva legato la validità giuridica della forma elettronica legandola esclusivamente alla tecnologia RSA, per di più rigorosamente attuata nelle regole dell'organizzazione di supporto.

Sulla base delle disposizioni sopra esaminate del « codice dell'amministrazione digitale » il diritto vigente italiano prevede una distinzione delle firme elettroniche in due grandi campi:

a) le firme digitali in senso strettamente giuridico: in Italia sono solo le firme qualificate; sono sempre valide e possono essere contestate solo fornendo la prova contraria sulla « paternità dell'atto »;

b) tutte le altre firme elettroniche riscontrabili nelle definizioni del « Codice » e nelle norme dispositive: vi rientrano tutte le ipotesi di cui ai nn. 2-3-4 della elencazione che segue. L'affidabilità dei documenti è rimessa per tutte alla libera valutazione del giudice.

Questa bipartizione discende dal fatto che alla firma digitale non qualificata non sono associati gli effetti giuridici di cui alla lettera a di cui sopra e neppure effetti giuridici intermedi, superiori a quelli delle firme di cui alla lettera *b*). Nelle norme dispositive si riscontrano accettazioni di documenti informatici in modi vari, che vanno separatamente considerati. L'opportunità di accompagnare alla bipartizione di cui sopra una classificazione più articolata discende dalla diversa rilevanza che possono assumere le differenti firme elettroniche in caso di contestazioni giudiziarie, ai sensi degli artt. 20 e 21 del « Codice ».

Possiamo quindi ribadire che il « Codice » ha accolto quattro categorie ben distinte di firme elettroniche. Le prime due accomunate dalla caratteristica di essere basate sulla tecnologia RSA; le altre accomunate dall'essere soluzioni tecniche legate all'accesso telematico. Per altro, solo la prima rientrante nella ipotesi *a*) di cui sopra e le altre tre riconducibili tutte alla ipotesi *b*):

---

[51] La nuova formulazione degli effetti della firma qualificata costituisce un miglioramento della disciplina che era contenuta nel TUDA, che attribuiva l'effetto di prova « fino a querela di falso »: soluzione giustamente criticata dalla dottrina: Masucci, *Documento informatico*, cit., p. 570-571.

1) nella prima categoria rientrano le soluzioni tecnologiche secondo le quali la firma si incorpora nel documento *in modo tecnicamente indissolubile*. Allo stato delle attuali tecnologie note l'unica ipotesi rientrante in questa categoria è la firma digitale. Sarebbero possibili variabili relative alla maggiore o minore complessità come numero dei bit del processo di criptazione[52], nonché dal punto di vista dell'organizzazione che fornisce i dispositivi ed i c.d. « certificati » e gestisce il sistema; il nostro diritto tuttavia riconosce piena efficacia soltanto ad un tipo di firma digitale che corrisponde ai massimi criteri di garanzia, disciplinati dal Codice della P.A. digitale: firme basate su certificato qualificato rilasciato da certificatore qualificato ai sensi degli allegati 1 e 2 della direttiva CE. Unica variabile ammessa è la provenienza dei dati per la firma e del relativo « certificato » da un certificatore accreditato. Il rigore alla base della differenza rispetto alla categoria seguente si desume, oltre che dalle definizioni *s*, *r* ed *f*, dall'art. 24 del « Codice », che ribadisce la necessità di un « certificato qualificato ».

2) Nella seconda categoria rientrano le firme RSA che non rispondono ai requisiti che il « Codice » richiede; si tratta delle « firme avanzate » di cui alla definizione 2 della direttiva CE: queste firme, in senso strettamente giuridico definitorio, non sono firme digitali, anche se tecnicamente basate sullo stesso metodo RSA (criptazione asimmetrica). Giuridicamente si tratta di più generiche firme elettroniche.

3) Nella terza categoria rientra invece una molteplicità di soluzioni tecnologiche, tutte consistenti comunque nella identificazione dell'operatore nel momento dell'accesso; l'accesso può portare alla creazione di documenti, ma questi non avranno nessuna caratteristica tecnica particolare[53] e non dovrebbe esserne possibile la libera circolazione in forma elettronica, salvo quanto sub 4.

4) Va infine considerata la documentazione validamente trasmessa ai sensi degli artt. 45, 47, 48 e 76. Forse il legislatore ha ecceduto nella semplificazione; comunque tutte queste norme si

[52] Il D.P.C.M. 13 gennaio 2004 recante le « Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici », al primo comma dell'art. 53 (« norme transitorie ») dispone che « In attesa della pubblicazione degli algoritmi per la generazione e verifica della firma digitale secondo quanto previsto dall'articolo 3, i certificatori accreditati ai sensi dell'articolo 28 del testo unico, devono utilizzare l'algoritmo RSA (Rivest-Shamir-Adleman) con lunghezza della chiave non inferiore a 1024 bit »; il richiamato art. 3 dispone al primmo comma che « I prodotti di firma digitale e i dispositivi sicuri di firma di cui all'articolo 29-*sexies* del testo unico, devono essere conformi alle norme generalmente riconosciute a livello internazionale o individuate dalla Commissione europea secondo la procedura di cui all'articolo 9 della direttiva n. 1999/93/Ce ». (http://www.interlex.it/Testi/dpc040113.htm); non risultano esistenti le norme europe attese, quindi si applica l'art. 53 del D.P.C.M.

[53] Come detto più sopra, dovrebbero essere archiviati su dischi WORM, ovvero salvati applicando una firma digitale della P.A., in funzione di validazione.

basano sulla verificabilità della provenienza e non richiedono necessariamente che vengano spediti documenti muniti di firma digitale.

Per quanto riguarda il riconoscimento ai fini dell'accesso, sorprende che il legislatore abbia completamente trascurato il metodo del riconoscimento biometrico ai fini delle firme elettroniche (unica menzione nell'art. 66, a proposito della carta d'identità elettronica); per la verità lo stesso TUDA menziona tre volte la biometria, ed in particolare nell'art. 22, definizione *e*, ma non collega alla possibilità tecnica particolari aspetti concretamente operativi. Anche il D.P.R. 513/97 conosceva l'identificazione a mezzo di chiavi biometriche, ma le norme tecniche non hanno utilizzato tale possibilità. La spiegazione va data considerando che, per quanto taluni riconoscimenti biometrici non siano particolarmente complessi e costosi, la loro concreta diffusione non è al momento prevedibile[54].

È opportuno sottolineare in queste conclusioni la soluzione giuridica che si è data al quesito relativo alla interrelazione tra gli artt. 20 e 21 e tutti gli altri esaminati nei §§ 6 e 7: *la contestabilità in giudizio delle firme non digitali*. Con questa interpretazione pensiamo che sia sensibilmente attenuato nella sostanza il divario di opinioni tra i sostenitori delle tesi rigoriste (« solo la RSA può essere una firma giuridicamente rilevante ») e la soluzione liberista che riscontriamo nel « Codice ».

Un'altra conclusione appare certa: lo sviluppo e la diffusione delle tecnologie richiederà periodici aggiornamenti delle fonti normative; sarebbe quindi opportuno che si differenziassero gli obbiettivi essenziali, inseriti in testi con forza di legge fondamentali, ma di limitata ampiezza, dalle norme di dettaglio di livello regolamentare, con ulteriore rinvio ai D.M. contenenti le vere e proprie norme tecniche.

Ultima osservazione: seduti ad un tavolino o in un laboratorio di ricerca si è in grado di sviluppare teorie di estrema raffinatezza e di prevedere soluzioni tecniche, funzionali e giuridiche intrinsecamente ineccepibili. La realtà, tuttavia, tende a scavalcare questi studi, accettando imperfezioni legate ad un pragmatismo non sempre criticabile, se realistico e se gli inconvenienti delle imperfezioni sono compensate da vantaggi quali la maggiore utilizzabilità e quindi la maggiore diffusione delle innovazioni. La soluzione della firma RSA è indubbiamente la migliore delle firme elettroniche ed

---

[54] Tra le utilizzazioni delle chiavi biometriche la più concreta sembra quella che condiziona la creazione della firma digitale al riconoscimento biometrico, in luogo (o in aggiunta) alla digitazione del PIN. In tal modo verrebbe eliminato l'unico difetto della firma RSA: l'uso abusivo da parte di chi non è titolare. Questa tecnologia dovrebbe essere comunque riservata alla redazione di documenti di particolare rilevanza: cfr.: DUNI, SIDDI, GERRA, GIACALONE, SANNA, cit.

è auspicabile che la sua diffusione si sviluppi il più possibile; se accompagnata dal riconoscimento biometrico al momento della generazione della firma si elimina anche il rischio dell'uso abusivo. Il legislatore, nelle varie disposizioni del « Codice », ha dato tuttavia ampio spazio ad una realtà digitale che solo in parte utilizza la firma digitale: per il resto accetta soluzioni già operative e le adotta in via temporanea e/o definitiva che lasciano spazio a riserve rispetto alla migliore tecnica della firma digitale. Si accetta cioè una realtà operativa nella quale l'effettività fisiologica funzioni nella stragrande maggioranza dei casi, relegando la patologia, le contestazioni e le controversie giudiziarie a casi rari e marginali. Una realtà basata sul reciproco affidamento, che in questo, come in tanti altri campi della vita umana, è alla base di tanti rapporti ed attività che altrimenti non esisterebbero neppure, se la diffidenza e la furbizia malevola fossero imperanti[55].

Comunque, in tutti i casi nei quali è necessario ricorrere alle più sicure garanzie della firma digitale qualificata, è quasi sempre indispensabile che il documento sia munito anche di marcatura temporale, ossia della certificazione della data (definizione *bb* dell'art. 1 del « Codice »): operazione possibile solo on line da parte del fornitore del servizio. La datazione certa è infatti indispensabile per due ordini di motivi: *a*) gli atti giuridici sono quasi sempre validi solo se compiuti entro i tempi che leggi specifiche prevedono; *b*) la stessa firma digitale ha una valenza predefinita e la sua validità va riscontrata con riferimento alla data del documento. Una firma potrebbe essere oggi scaduta, ma poteva essere valida alla data del documento. Viceversa una firma potrebbe essere valida oggi, ma non alla data trascorsa che si vorrebbe attribuire al documento (che, nel caso che si ipotizza, è esibito privo di marcatura temporale).

APPENDICE

Dir. 13 dicembre 1999 n. 93. *Direttiva del Parlamento europeo e del Consiglio relativa ad un quadro comunitario per le firme elettroniche*. Pubblicata nella G.U.C.E. 19 gennaio 2000, n. L 13. Entrata in vigore il 19 gennaio 2000.

Articolo 2. (*Definizioni*). — Ai fini della presente direttiva, valgono le seguenti definizioni:

1) « firma elettronica », dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazione[56];

---

[55] Si pensi ai sistemi di commercio elettronico del tipo di e-Bay, nel quale chiunque può entrare senza referenze iniziali; opportunamente il sistema prevede l'acquisizione progressiva di referenze positive e negative di ogni soggetto venditore, ma, inizialmente, ognuno opera sulla base di un affidamento che normalmente da esiti positivi.

[56] Si ritiene opportuno riportare qui appresso il testo inglese: 1. « electronic si-

2) « firma elettronica avanzata », una firma elettronica che soddisfi i seguenti requisiti:

a) essere connessa in maniera unica al firmatario;

b) essere idonea ad identificare il firmatario;

c) essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;

d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati;

3) « firmatario », una persona che detiene un dispositivo per la creazione di una firma e agisce per conto proprio o per conto della persona fisica o giuridica o dell'entità che rappresenta;

4) « dati per la creazione di una firma », dati peculiari, come codici o chiavi crittografiche private, utilizzati dal firmatario per creare una firma elettronica;

5) « dispositivo per la creazione di una firma », un software configurato o un hardware usato per applicare i dati per la creazione di una firma;

6) « dispositivo per la creazione di una firma sicura », un dispositivo per la creazione di una firma che soddisfa i requisiti di cui all'allegato III;

7) « dati per la verifica della firma », dati, come codici o chiavi crittografiche pubbliche, utilizzati per verificare una firma elettronica;

8) « dispositivo di verifica della firma », un software configurato o un hardware usato per applicare i dati di verifica della firma;

9) « certificato », un attestato elettronico che collega i dati di verifica della firma ad una persona e conferma l'identità di tale persona;

10) « certificato qualificato », un certificato conforme ai requisiti di cui all'allegato I e fornito da un prestatore di servizi di certificazione che soddisfa i requisiti di cui all'allegato II;

11) « prestatore di servizi di certificazione », un'entità o una persona fisica o giuridica che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche;

12) « prodotto di firma elettronica », hardware o software, oppure i componenti pertinenti dei medesimi, destinati ad essere utilizzati da un prestatore di servizi di certificazione per la prestazione di servizi di firma elettronica oppure per la creazione o la verifica di firme elettroniche;

13) « accreditamento facoltativo », qualsiasi permesso che stabilisca diritti ed obblighi specifici della fornitura di servizi di certificazione, il quale sia concesso, su richiesta del prestatore di servizi di certificazione interessato, dall'organismo pubblico o privato preposto all'elaborazione e alla sorveglianza del rispetto di tali diritti ed obblighi, fermo restando che il prestatore di servizi di certificazione non è autorizzato ad esercitare i diritti derivanti dal permesso fino a che non abbia ricevuto la decisione da parte dell'organismo.

....

Articolo 5. (*Effetti giuridici delle firme elettroniche*). — 1. Gli Stati membri provvedono a che le firme elettroniche avanzate basate su un certificato qualificato e create mediante un dispositivo per la creazione di una firma sicura:

a) posseggano i requisiti legali di una firma in relazione ai dati in forma elettronica così come una firma autografa li possiede per dati cartacei; e

b) siano ammesse come prova in giudizio.

2. Gli Stati membri provvedono affinché una firma elettronica non sia considerata legalmente inefficace e inammissibile come prova in giudizio unicamente a causa del fatto che è: — in forma elettronica, o — non basata su un certificato qualificato, o — non basata su un certificato qualificato rilasciato da un prestatore di

---

gnature » means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication ».

servizi di certificazione accreditato, ovvero — non creata da un dispositivo per la creazione di una firma sicura.

D. Lgs. 7 marzo 2005, n. 82. ***Nella versione modificata dal D. Legisl. 4 aprile 2006, n. 159.***

Articolo 1. (*Definizioni*). — 1. Ai fini del presente codice si intende per:

a) allineamento dei dati: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;

b) autenticazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;

c) carta d'identità elettronica: il documento d'identità munito di fotografia del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare;

d) carta nazionale dei servizi: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;

e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;

f) certificato qualificato: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciato da certificatore che risponde ai requisiti di cui all'allegato II della medesima direttiva;

g) certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

i) chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;

l) dato a conoscibilità limitata: il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;

m) dato delle pubbliche amministrazioni: il dato formato, o comunque trattato da una pubblica amministrazione;

n) dato pubblico: il dato conoscibile da chiunque;

o) disponibilità: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge;

p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

q) 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;

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

s) firma digitale: un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

t) fruibilità di un dato: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;

u) gestione informatica dei documenti: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;

v) originali non unici: 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;

z) pubbliche amministrazioni centrali: le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;

aa) titolare: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;

bb) validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

Capo II. Documento informatico e firme elettroniche; pagamenti, libri e scritture

Sezione I. Documento informatico

Articolo 20. (*Documento informatico*). — 1. Il documento informatico da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice;

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

2. Il documento informatico sottoscritto con firma elettronica qualificata o con firma digitale, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, si presume riconducibile al titolare del dispositivo di firma ai sensi dell'articolo 21, comma 2, e soddisfa comunque il requisito della forma scritta, anche nei casi previsti, sotto pena di nullità, dall'articolo 1350, primo comma, numeri da 1 a 12 del codice civile.

3. Le regole tecniche per la formazione, trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici sono stabilite ai sensi dell'articolo 71; la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.

5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.

Articolo 21. (*Valore probatorio del documento informatico sottoscritto*). — 1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia la prova contraria.

3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:

a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del 13 dicembre 1999 del Parlamento europeo e del Consiglio, ed è accreditato in uno Stato membro;

b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;

c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

Articoolo 23. (*Copie di atti e documenti informatici*). — 1. All'articolo 2712 del codice civile dopo le parole: « riproduzioni fotografiche » è inserita la seguente: « , informatiche ».

2. I duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge, se conformi alle vigenti regole tecniche.

2-*bis*. Le copie su supporto cartaceo di documento informatico, anche sottoscritto con firma elettronica qualificata o con firma digitale, sostituiscono ad ogni effetto di legge l'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

3. I documenti informatici contenenti copia o riproduzione di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata.

4. Le copie su supporto informatico di documenti originali non unici formati in origine su supporto cartaceo o, comunque, non informatico sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è assicurata dal responsabile della conservazione mediante l'utilizzo della propria firma digitale e nel rispetto delle regole tecniche di cui all'articolo 71.

5. Le copie su supporto informatico di documenti, originali unici, formati in origine su supporto cartaceo o, comunque, non informatico sostituiscono, ad ogni effetto di legge, gli originali da cui sono tratte se la loro conformità all'originale è autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.

6. La spedizione o il rilascio di copie di atti e documenti di cui al comma 3, esonera dalla produzione e dalla esibizione dell'originale formato su supporto cartaceo quando richieste ad ogni effetto di legge.

7. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71 di concerto con il Ministro dell'economia e delle finanze.

Capo IV. Trasmissione informatica dei documenti

Articolo 45. (*Valore giuridico della trasmissione*). — 1. I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, ivi compreso il fax, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

Articolo 47. (*Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni*). — 1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono di norma mediante l'utilizzo della posta elettronica; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

2. Ai fini della verifica della provenienza le comunicazioni sono valide se:

a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;

b) ovvero sono dotate di protocollo informatizzato;

c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71;

d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

3. Entro otto mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni centrali provvedono a:

a) istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, per ciascun registro di protocollo;

b) utilizzare la posta elettronica per le comunicazioni tra l'amministrazione ed i propri dipendenti, nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

Articolo 48. (*Posta elettronica certificata*). — 1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

2. La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta.

3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso mediante posta elettronica certificata sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche.

Articolo 76. (*Scambio di documenti informatici nell'ambito del Sistema pubblico di connettività*). — 1. Gli scambi di documenti informatici tra le pubbliche amministrazioni nell'ambito del SPC, realizzati attraverso la cooperazione applicativa e nel rispetto delle relative procedure e regole tecniche di sicurezza, costituiscono invio documentale valido ad ogni effetto di legge .

Articolo 64. (*Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni*). — 1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica.

2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'autenticazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano di accertare l'identità del soggetto che richiede l'accesso. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

3. Ferma restando la disciplina riguardante le trasmissioni telematiche gestite dal Ministero dell'economia e delle finanze e dalle agenzie fiscali, con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, è fissata la data, comunque non successiva al 31 dicembre 2007, a decorrere dalla quale non è più consentito l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni, con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi. È prorogato alla medesima data il termine relativo alla procedura di accertamento preventivo del possesso della Carta di identità elettronica (CIE), di cui all'articolo 8, comma 5, del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, limitatamente alle richieste di emissione di Carte nazionali dei servizi (CNS) da parte dei cittadini non residenti nei comuni in cui è diffusa la CIE.

Articolo 65. (*Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica*). — 1. Le istanze e le dichiarazioni presentate alle pubbliche amministrazioni per via telematica ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:

a) se sottoscritte mediante la firma digitale, il cui certificato è rilasciato da un certificatore accreditato;

b) ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;

c) ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente e fermo restando il disposto dell'articolo 64, comma 3.

2. Le istanze e le dichiarazioni inviate o compilate su sito secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento; resta salva la facoltà della pubblica amministrazione di stabilire i casi in cui è necessaria la sottoscrizione mediante la firma digitale.

3. Dalla data di cui all'articolo 64, comma 3, non è più consentito l'invio di istanze e dichiarazioni con le modalità di cui al comma 1, lettera *c*).

4. Il comma 2 dell'articolo 38 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è sostituito dal seguente:

« 2. Le istanze e le dichiarazioni inviate per via telematica sono valide se effettuate secondo quanto previsto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82 ».