LA NATURA GIURIDICA DEI CERTIFICATORI NEL SISTEMA DI FIRMA DIGITALE – IPOTESI DI RESPONSABILITA' PENALE

di

Marco Scialdone

Sommario

INTRODUZIONE

La diffusione delle tecnologie informatiche ed il conseguente sviluppo della società dell'informazione hanno aumentato esponenzialmente il numero delle attività che si svolgono a distanza così da risultare, oggigiorno, ampiamente comuni rapporti commerciali o istituzionali tra individui che non si sono mai incontrati fisicamente.

In tutto questo emerge sempre più pressante la necessità del riconoscimento sicuro dei soggetti interconnessi, dell'autenticità dei contenuti e del valore legale dei documenti digitali, ai quali non è possibile apporre firme, timbri e altri strumenti tradizionali di validazione, nella loro accezione tradizionale.

Il nostro paese è stato il primo ad affrontare siffatto problema con una visione sistematica proiettata al futuro: invece di adottare disposizioni limitate a determinati ambienti ed a determinate transazioni si è cercato di costruire un ponte di collegamento tra la tecnologia ed il diritto, stabilendo i requisiti che il documento informatico deve presentare per avere piena rilevanza e validità legale, alla pari con il documento tradizionale.

Finalità del presente saggio non è quella di operare una ricostruzione storico-normativa della validità giuridica del documento informatico nell'ordinamento italiano quanto di prendere in considerazione un particolare aspetto, quello relativo al documento informatico sottoscritto con firma digitale, per esplorare

i profili relativi alla natura giuridica e conseguentemente alla responsabilità penale che possano configurarsi in capo ai soggetti che la normativa in materia definisce quali “certificatori” e che rappresentano la vera novità, la vera rivoluzione, prima di tutto culturale, rispetto a ciò che, nella percezione comune, si associa alla sottoscrizione autografa di un documento.

Il percorso che, a parere di chi scrive, merita di essere seguito per una trattazione chiara ed satisfattiva non può che partire da una descrizione, sia pure sommaria, di cosa sia la firma digitale.

Una volta comprese le caratteristiche di quest'ultima, si potrà affrontare con maggiore cognizione la problematica relativa alla definizione ed al ruolo dei certificatori nel nostro sistema ed infine procedere ad una valutazione dei profili di responsabilità penale che possano ravvisarsi nell'attività da essi espletata.

1.1 LA FIRMA DIGITALE

L'art. 1 del D.P.R. 445/2000, come modificato dal D.P.R. 137/2003, definisce la firma digitale come “un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, pubblica e privata, che consente al titolare tramite la chiave privata ed 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” (la definizione è stata mantenuta inalterata anche nel nuovo Codice dell’Amministrazione Digitale – D.lgs 82/2005 – che entrerà in vigore dal 1 Gennaio 2006, sostituendo l’attuale impianto normativo).

La stessa disposizione chiarisce cosa debba intendersi per firma elettronica qualificata, di cui la firma digitale è species: la firma elettronica qualificata è una firma elettronica avanzata [1]basata su un certificato qualificato e creata mediante un dispositivo sicuro di firma (su quest’ultima definizione è destinata ad incidere l’entrata in vigore del Codice sopra richiamato. In esso, infatti, scompare qualsiasi riferimento alla “firma elettronica avanzata”, la cui

1Ai sensi dell'articolo 2, comma 1, lett. g) d.lgs. 10/2002 la firma elettronica avanzata è la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

definizione – vedi nota 1 – è sostanzialmente trasfusa in quella di “firma elettronica qualificata”).
Ecco allora che, sulla base delle disposizioni sopra riportate siamo in grado di comprendere come funzioni la firma digitale, cioè come si può dare ad un testo chiaro la certezza dell'identità del firmatario e dell'integrità del contenuto.
Innanzitutto il cifrario asimmetrico: esso è fondato sull'uso di due chiavi diverse, generate insieme nel corso di un unico procedimento. Una delle due chiavi serve per cifrare (chiave diretta) ed una per decifrare (chiave inversa).
Le proprietà fondamentali di un tale sistema sono:

- non si può decifrare il testo con la stessa chiave usata per cifrarlo;
- le due chiavi sono generate con la stessa procedura e correlate univocamente;
- conoscendo una delle due chiavi non c'è nessun modo di ricostruire l'altra.

In tal guisa una delle due chiavi può essere resa pubblica, mentre l'altra deve essere tenuta segreta.
A questo punto il sistema più elementare per garantire al terzo la provenienza e l'integrità del documento sarebbe quello di inviargli un testo chiaro insieme ad una versione dello stesso cifrata con la chiave privata del mittente. Il destinatario sarebbe chiamato a decifrare il testo con la chiave pubblica del mittente e, se i due testi risultano uguali, ottiene le due certezze sull'identità del mittente e sull'integrità del contenuto.

Tuttavia un sistema del genere sarebbe lento, perchè risulterebbe necessario cifrare e decifrare tutto il documento, operazione potenzialmente molto lunga e strettamente connessa alla potenza dell'elaboratore utilizzato.

Per ovviare ad un simile inconveniente si ricorre allora ad una semplificazione che consiste nel cifrare solo un brevissimo riassunto del testo stesso, ottenuto con una procedura detta funzione di *hash*: pochi caratteri che costituiscono l'impronta del testo.

Se alla fine della procedura l'impronta che risulta dalla decifratura con la chiave pubblica del mittente è uguale a quella che si ottiene applicando la funzione di hash al testo chiaro, vuol dire che esso proviene da chi appare come il titolare della chiave pubblica e che non è stato alterato dopo la generazione della firma digitale.

In tutto quanto delineato c'è un punto essenziale che è dato dalla conoscibilità della chiave pubblica, con il corollario della sua attendibilità.

Se la comunicazione si deve svolgere tra due soggetti che si conoscono, essi possono direttamente scambiarsi le rispettive chiavi pubbliche. Ma il grande vantaggio dei sistemi di crittografia a chiave asimmetrica è proprio la possibilità di rendere pubblica una delle due chiavi, consentendo a chiunque di controllare che un messaggio provenga proprio dal titolare dell'altra chiave, quella privata, e che non sia stato alterato o contraffatto.

Naturalmente la pubblicazione ed il controllo delle chiavi si svolgono per via telematica, accedendo ad appositi registri, che costituiscono il punto critico del sistema.

Infatti è indispensabile che i gestori di questi registri siano soggetti

assolutamente scrupolosi e fidati e, in qualche modo, a loro volta, certificati. Altrimenti sarebbe molto facile per un malintenzionato pubblicare una chiave facendosi passare per un altro o contraffare chiavi altrui, con o senza la complicità del gestore del registro, con il risultato che dalla massima sicurezza consentita dalla crittografia a chiave asimmetrica si passi alla massima insicurezza che deriva dalla malafede, o più semplicemente dalla negligenza, aggravate dall'impossibilità di distinguere i bit veri da quelli falsi.

Dunque in tutto il processo della firma digitale è necessario l'intervento di una "terza parte fidata" (*trusted third part*), generalmente nota come ***Certification Authority*** (nel nostro ordinamento "il certificatore").

Nello schema teorico della firma digitale c'è una distinzione tra CA (***Certification Authority***) e RA (***Registration Authority***): la prima ha il compito di gestire il database delle chiavi pubbliche e dei relativi certificati delle chiavi, la seconda ha la responsabilità di procedere all'identificazione del soggetto che richiede la certificazione.

Questo sdoppiamento è stato rifiutato dal legislatore italiano che ha voluto unificare in un unico soggetto (il certificatore) tutte le responsabilità derivanti dall'esercizio della certificazione con l'evidente vantaggio di offrire al consumatore-utente una maggiore tutela.

L'insieme costituito dai soggetti indicati (utente, certificatore, destinatario ecc.), il modo con il quale ciascuno di essi assolve il proprio ruolo e le modalità di utilizzazione delle tecnologie disponibili, costituisce la **PKI** (***Public Key Infrastructure***),

l'infrastruttura di chiave pubblica.

Nel presente elaborato ci si soffermerà nel seguito, su uno degli attori di tale infrastruttura; il certificatore.

Si analizzerà, come accennato in precedenza, innanzitutto il ruolo del certificato nel sistema di firma digitale, alla luce della normativa nazionale, per passare poi ad un'analisi delle caratteristiche dei soggetti preposti all'attività di certificazione così da farne emergere profili di responsabilità penale scaturenti ed intimamente connessi alla loro qualificazione giuridica.

1.2 I CERTIFICATI

I certificati sono documenti elettronici rilasciati dai certificatori che riassumono, in buona sostanza, i dati identificativi del titolare e contengono una serie variabile di informazioni atte a consentire principalmente di rendere noto il soggetto che li ha emessi e le modalità per la verifica di validità del certificato.
Più precisamente, in funzione del loro contenuto, secondo la definizione dell'art. 1 del DPR 137/2003, essi si possono distinguere in:

- Elettronici: ai sensi dell'art. 2, comma 1, lettera d), del decreto legislativo 23 gennaio 2002, n. 10, sono gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi;
- Qualificati: ai sensi dell'art. 2, comma 1, lettera e), del decreto legislativo 23 gennaio 2002, n. 10, sono i certificati elettronici conformi ai requisiti indicati nell'Allegato I della Direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti dell'Allegato II della medesima

direttiva.

Come evidente esiste una duplice possibilità: la prima non strutturata, che lascia ampia libertà di scelta nei contenuti al certificatore. La seconda, più strutturata, maggiormente rivolta ad assicurare un livello di qualità delle informazioni fornite e quindi più adatta a garantire sicurezza nell'utilizzo. La differenza tra le due tipologie di certificati è importante, in quanto solo la tipologia "certificato qualificato" è in grado, se combinata opportunamente con altri presupposti, di garantire il massimo livello di efficacia di una firma elettronica.
In particolare, ad evidenti fini di sicurezza, la struttura del contenuto dei certificati qualificati è determinata dall'articolo 27 del DPR 445/2000 (come modificato dal DPR 137/2003) – dal 1 gennaio 2006, art. 28, D.lgs 82/2005 - il quale prevede specificatamente che i certificati qualificati devono contenere almeno le seguenti informazioni:

- Indicazione che il certificato elettronico rilasciato è un certificato qualificato;
- Numero di serie o altro codice identificativo del certificato;
- Nome, ragione o denominazione sociale del certificatore e lo stato nel qual è stabilito;
- Nome, cognome e codice fiscale del titolare del certificato o uno pseudonimo chiaramente identificato come tale;
- Dati per la verifica della firma corrispondenti ai dati per la

creazione della stessa in possesso del titolare;

- Indicazione del termine iniziale e finale del periodo di validità del certificato;
- Firma elettronica avanzata (nel nuovo codice dell'Amministrazione Digitale, scomparso il riferimento alla firma elettronica avanzata, si parla di Firma elettronica qualificata) del certificatore che ha rilasciato il certificato.

Dunque un certificato potrà dirsi qualificato qualora presenti una struttura che contenga almeno i contenuti sopra indicati. Eventuali deviazioni da tale contenuto minimo determinerebbero la perdita della qualità di certificato qualificato.

1.3 I CERTIFICATORI

I certificatori vengono definiti dal D. lgs 10/2002 (e allo stesso modo dal Codice dell?amministrazione Digitale) quali soggetti pubblici o privati che svolgono “servizi di certificazione delle firme elettroniche o forniscono altri servizi ad esse connessi; rilasciano, revocano o sospendono i certificati”. Ad essi è attribuita la possibilità di svolgere i c.d. “servizi connessi” al servizio di certificazione, tra cui si individuano, ai sensi di quanto stabilito dalla Direttiva 1999/93/CE: immatricolazione; validazione temporale; repertorizzazione; servizi informatici o di consulenza relativi alle firme elettroniche.

In base all’art. 3 del D.lgs. 10/2002 (art. 26, D.Lgs 82/2005), ed in ottemperanza ad un principio generale introdotto dalla citata Direttiva, la prestazione dei servizi di certificazione è libera e non subordinata ad autorizzazione preventiva; nemmeno il numero dei certificatori può essere limitato.

Poiché la direttiva ammette la creazione di sistemi di accreditamento come strumento per il miglioramento del livello di servizio ed accrescere la fiducia degli utilizzatori dei servizi e più in generale la sicurezza e qualità degli stessi, e stabilisce un generale principio di libertà di adesione per quei certificatori che ritengono di trarne vantaggio, il D. lgs 10/2002 ha introdotto con l’art. 5 la

possibilità, per i certificatori che effettuino un scelta in tal senso, di ottenere il riconoscimento del più elevato livello in termini di qualità e sicurezza.
In particolare i certificatori si dividono in:

- CERTIFICATORE: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;
- CERTIFICATORE QUALIFICATO: il certificatore che rilascia al pubblico certificati elettronici conformi ai requisiti indicati nel DPR 445/2000 e nelle regole tecniche di cui all'art. 8, comma 2 del medesimo provvedimento (ai certificatori qualificati è dedicato l'art. 27 del D.lgs 82/2005).
- CERTIFCATORE ACCREDITATO: il certificatore accreditato in Italia ovvero in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE, nonché ai sensi del DPR 445/2000 (ai certificatori qualificati è dedicato l'art. 28 del D.lgs 82/2005);

Per quanto riguarda i requisiti richiesti, l'articolo 26 del DPR 445/2000 (come modificato dal DPR 137/2003) – così pure l'art. 26 del D.lgs 82/2005 - stabilisce ora che i "certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo

unico delle leggi in materia bancaria e creditizia, approvato con decreto legislativo 1 settembre 1993, n. 385."

L'eventuale accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività di impresa.

Da notare che ai certificatori qualificati ed ai certificatori accreditati che hanno sede stabile in altri Stati membri dell' Unione europea non si applicano le norma del DPR 445/2000 e le relative norme tecniche di cui all'articolo 8, comma 2, del medesimo testo unico e si applicano in sostituzione le rispettive norme di recepimento della direttiva 1999/93/CE.

Con specifico riferimento ai Certifcatori qualificati l'articolo 27 del DPR 445/2000 – idem l'art. 27 del D.lgs 82/2005 - prevede che essi debbano inoltre:

- Dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;
- Impiegare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate, e che sia in grado di rispettare le norme del presente testo unico e le regole tecniche di cui all'articolo 8, comma 2;
- Applicare procedure e metodi amministrativi e di gestione

adeguati e tecniche consolidate;

- Utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo ed internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 10, comma 1, del decreto legislativo 23 Gennaio 2002, 10;
- Adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi, nei casi in cui il certificatore generi tali chiavi.

I certificatori cd. "accreditati" sono invece soggetti che emettono certificati qualificati e che hanno ottenuto il riconoscimento del possesso dei requisiti del livello più elevato in termini di qualità e sicurezza, nonché in ordine alla solidità finanziaria ed alla onorabilità; sono soggetti al controllo preventivo prima dell'accreditamento nonché alla vigilanza da parte del Dipartimento dell'innovazione e le tecnologie presso la Presidenza del Consiglio dei Ministri, anche tramite strutture delegate.

I certificatori cd. "notificati" (o qualificati) sono invece tutti i soggetti che, pur emettendo certificati qualificati, non presentato i più elevati requisiti di sicurezza e qualità, anche tecnica ed economica, che caratterizzano i certifcatori accreditati; come detto, essi devono, prima dell'inizio della loro attività, effettuare idonea comunicazione al Dipartimento per l'innovazione e la tecnologia e

sono soggetti a vigilanza da parte di quest'ultimo.

Come si nota il legislatore italiano, in conformità alle indicazioni della direttiva 1999/93/CE, ha stabilito un principio generale di libertà di forme e di requisiti, salvo stabilire requisiti particolari per i certificatori qualificati e più ancora accreditati, attribuendo ai certificati emessi da tali soggetti una valenza particolare.

E' sin troppo intuitivo osservare come la differenza tra le varie tipologie di certificatori sia costituita dai requisiti di qualità e di sicurezza. In particolare, per i certificatori accreditati, il legislatore precisa che la procedura preventiva a cui vengono sottoposti consiste appunto nell'accertamento del più elevato livello di qualità e sicurezza.

1.4 LA NATURA GIURIDICA DEI CERTIFICATORI

Preliminarmente si può dire che il ruolo del certificatore è sicuramente di interesse pubblico: pur essendo venuto meno il previgente obbligo normativo di iscrizione in un apposito elenco per l'esercizio dell'attività di certificazione, è comunque vero che senza l'opera di tali soggetti il cittadino non può firmare il documento con uno strumento di firma digitale e realizzare la conseguente efficacia probatoria prevista dalla legge.

Tutto ciò evidenzia comunque un importante "ruolo pubblicistico" dei soggetti certificatori [2].

Occorre dunque interrogarsi se essi possano, nel nostro ordinamento, qualificarsi quali pubblici ufficiali, o persone incaricate di pubblico servizio o, ancora, esercenti un servizio di pubblica necessità.

Non è possibile riportare in questa sede tutte le diatribe dottrinarie sui requisti che distinguono siffatte figure[3]: partiamo invece dalle disposizioni codicistiche per cercare di impostare in modo corretto la relativa problematica.

2Vedi C. Sarzana di S. Ippolito, *Documento informatico, firma digitale e crittografia. Riflesioni giuridiche e penalistiche, in* Atti convegmo ITA " *La firma elettronica e le regole tecniche*", Roma 15 – 16 luglio 1999, pp 7 ss.

3Si veda per una sintesi ed un'esaustiva bibliografia, Antolisei F., Manuale di Diritto penale Parte specialeII GIUFFRE'.

Art. 357 c.p. - Nozione di Pubblico Ufficiale

“Agli effetti della legge penale, sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi, e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di ***poteri autoritativi o certificativi.****”*

Art. 358 c.p. - Nozione della persona incaricata di un pubblico servizio

“Agli effetti della legge penale, sono incaricati di pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un’attività disciplinata mele stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest’ultima, e con l’esclusione dello svolgimento di semplici mansioni d’ordine e della prestazione di opera meramente materiale.”

Art. 359 c.p. - Persone esercenti un servizio di pubblica necessità.

“Agli effetti della legge penale, sono persone che esercitano un servizio di pubblica necessità:

1) *i privati che esercitano professioni forensi o sanitarie, o altre professioni il cui esercizio sia per la legge vietato senza una speciale abilitazione dello Stato, quando dell’opera di essi il pubblico sia per legge obbligato a valersi;*

2) *i privati che, non esercitando una pubblica funzione, né prestando un pubblico servizio. Adempiono un servizio dichiarato di pubblica necessità mediante un atto della pubblica Amministrazione.”*

Dalle definizioni sopra riportate e dal quadro normativo in precedenza delineato si può senz'altro escludere che i certificatori siano soggetti esercenti un servizio di pubblica necessità: in base all’art. 3 del D.lgs. 10/2002, ed in ottemperanza ad un principio generale introdotto dalla Direttiva 1999/93/CE – principio confermato, come detto nel nuovo Codice dell’Amministrazione Digitale -, la prestazione dei servizi di certificazione è libera e non subordinata ad autorizzazione preventiva; nemmeno il numero dei certificatori può essere limitato.

Né si potrebbe argomentare diversamente con riferimento alle categorie dei certificatori “notificati” o “accreditati” poiché nel primo caso la notificazione effettuata all'autorità competente pur

precedendo l'inizio dell'attività non è subordinata al conseguimento di “una speciale abilitazione”, consistendo in un mero atto dichiarativo, mentre nel secondo, se è vero che il controllo è preventivo e dunque si potrebbe configurare il requisito della “speciale abilitazione da parte dello Stato” per l'esercizio dell'attività, è altrettanto vero che dell'opera di questi ultimi il cittadino non è obbligato ad avvalersi, rappresentando una mera opzione per così dire “qualitativa” rispetto ad altra disponibile sul mercato e comportante il raggiungimento dei medesimi risultati.

La natura dei certificatori quali esercenti un servizio di pubblica necessità era stata sostenuta[4] in dottrina allorquando, vigente un diverso quadro normativo, per diventare certificatore c'era bisogno dell'iscrizione in un apposito elenco, la cui cura era affidata all'AIPA che, pur quasi senza l'ausilio di discrezionalità, ammetteva o meno gli aspiranti certificatori.

La stessa dottrina sopra richiamata[5] aveva invece così liquidato la possibilità che essi avessero natura di pubblici ufficiali: “sicuramente il certificatore, come soggetto privato, non è un pubblico ufficiale”.

Ebbene, la Suprema Corte ha messo almeno un punto fisso in questa complicata materia: il solo fatto di essere un soggetto privato non esclude il poter rivestire la funzione di pubblico ufficiale.

Si rimanda alla lettura delle varie sentenze[6] in tal senso, riportando solo la più esaustiva e chiarificatrice:

4Parodi C., Calice A., *Responsabilità penali e Internet*, IL SOLE 24 ORE, pp. 163 ss.
5Parodi C., op. cit.
6Cass- Pen 2583/96, 421/96, 3882/97, sez. un. 11.7.1992.

“La natura privatistica... non è di per sé rilevante ad escludere la qualità di pubblico ufficiale o di incaricato di pubblico servizio, ben potendo non solo il pubblico servizio, ma anche la pubblica funzione essere esercitate da un privato”[7]

Peraltro la stessa Corte di Cassazione ha escluso la rilevanza di un provvedimento concessorio al fine della qualificazione di un'attività come servizio pubblico[8]

Dunque ai fini della riconducibilità o meno del certificatore alla nozione di pubblico ufficiale ex art. 357 c.p. bisogna valutare i soli criteri che forniti dalla legge e dalla giurisprudenza: potestà d'imperio e/o di certificazione[9], interesse della collettività[10], regolamentazione dell'attività in forma pubblicistica.

La funzione pubblica, inoltre, non è esclusa per funzioni sussidiarie o accessorie a quelle istituzionali. In ultima analisi potrebbe giovare la comparazione dei requisiti societari dei certificatori con quelli delle banche, considerate per certi compiti facenti funzioni pubbliche.

Merita di essere riportato quanto sostenuto dall'Antolisei[11] in merito alla questione di cui si sta trattando:

7Cass. Pen. 793/96
8Cass. Pen. 793/96
9Cass Pen VI 5.2.1991 e 26.2.1993
10Per i soli incaricati di pubblico servizio basterebbe solo questo criterio secondo Cass. 10735/96.
11Antolisei F., Manuale di Diritto penale Parte specialeII, pag. 278, GIUFFRE’.

“Accanto alla larga classe delle persone che formano o concorrono a formare la volontà dell'ente pubblico o in qualsiasi modo lo impersonano di fronte agli estranei, la qualifica di pubblico ufficiale va riconosciuta a due altre categorie di individui:

1. *coloro che sono munti di poteri autoritativi...*
2. *coloro che sono muniti di poteri di certificazione, vale a dire l persone che hanno la facoltà di rilasciare documenti che nel nostro ordinamento giuridico hanno efficacia probatoria...*

Il nuovo testo dell'art. 357 ha ciò riconosciuto quando ha accennato a quella caratteristica della funzione amministrativa che è il suo svolgersi per mezzo di poteri autoritativi o certificativi”

Giova ricordare che, sempre secondo lo stesso Autore, “tutte le persone investite di mansioni di interesse pubblico che non appartengano alla categoria degli esercenti un servizio di pubblica necessità vanno considerate come incaricati di pubblico servizio”.

Alla luce di quanto fin qui esposto, a parere di scrive, sembra sostenibile poter qualificare i certificatori quali pubblici ufficiali, proprio sulla base di quel potere certificatorio loro attribuito dall'ordinamento.

De resto come considerare un servizio semplicemente privato l'identificazione dei cittadini, la gestione di un registro dei certificati

rilasciati imposto dalla legge ed obbligatoriamente accessibile al pubblico?

Il Miccoli[12], pur non affrontando direttamente la questione, sembra voler considerare un vero e proprio pubblico registro quello tenuto dai certificatori, al pari della Conservatoria dei Registri Immobiliari, del Registro delle Imprese, delle Matricole delle navi maggiori ecc.

Sembra ragionevole aderire ad una simile impostazione: la firma digitale ha determinato un cambiamento che è innanzitutto culturale.

Mentre la firma autografa di un individuo è sempre uguale a se stessa, la firma digitale è sempre diversa, perchè viene di volta in volta generata a partire dal contenuto del documento.

Si può dire che mentre la firma autografa è orientata all'individuo, la firma digitale è orientata al documento.

Questo innesca dinamiche giuridiche del tutto nuove, prima fra tutte l'esigenza di un soggetto, terza parte fidata, che attesti la nostra identità, attesti in sostanza “chi siamo”.

Mentre nei sistemi tradizionali di firma è la calligrafia a farsi portavoce e garante della nostra identità, il carattere inevitabilmente neutro dei bit pone un'esigenza ulteriore che è quella legata all'identificazione del soggetto firmatario.

Ed ancora: senza l'intervento del certificatore non è possibile firmare digitalmente un documento informatico, senza quell'intervento si può a ragione sostenere che l'individuo è privato della sua stessa identità di fronte a terzi, una privazione che diventa

12 Miccoli, *Documento e commercio telematico*, IPSOA 1998

assoluta nei rapporti che egli intrattiene per via esclusivamente telematica; un'identità che può essergli negata o peggio ancora misconosciuta, alterata, laddove quell'attività di certificazione avvenga in modo intenzionalmente inesatto o lacunoso.

Certamente la qualificazione dei certificatori come pubblici ufficiali graverebbe questi soggetti di responsabilità robuste, ma anche, giova ricordarlo, di una tutela più ampia.

Occorre, infatti, partire dalla considerazione che la qualifica di pubblico ufficiale, nel nostro ordinamento penale, da una parte è destinata a sancire a carico del titolare una più grave responsabilità per l'infrazione dei doveri che gli incombono, dall'altra ad assicurare allo stesso una più energica tutela.

Quest'ultimo aspetto non è da sottovalutare: l'utente sapendo di avere a che fare con un pubblico ufficiale sarebbe sicuramente più restio a rilasciare dichiarazioni false, considerata la più gravosa responsabilità penale.

Anche coloro che fossero intenzionati ad attacchi di tipo informatico riceverebbero sicuramente una risposta più robusta da parte dell'ordinamento: ad esempio, *ex* art. 420c.p., gli impianti telematici dei certificatori sarebbero di certo considerati di pubblica utilità.

Certamente *ubi lex voluit ibi dixit*, eppure, per citare un esempio emblematico, i compilatori di documenti che accompagnano i prodotti vitivinicoli non credevano di essere pubblici ufficiali fino a quando la Cassazione ha avuto modo di pronunciarsi in tal senso[13].

13Cass. Pen 1357/86

Passando poi a considerazioni meno giuridiche, la qualificazione di pubblici ufficiali dei certificatori gioverebbe alla diffusione della firma digitale.

Se si pensa che, in futuro non troppo lontano, milioni di italiani faranno uso della firma digitale nelle loro transazioni quotidiane, si capisce come la questione diventi molto importante per la fiducia del cittadino, il quale affiderà la propria identità in rete a tali soggetti.

Forse dunque, sarebbe d'uopo, un intervento chiarificatore del legislatore, tenuto conto di quanto si è andato dicendo finora in merito al ruolo di “garante” dell'identità telematica di milioni di persone che i certificatori sono e saranno chiamati a svolgere.

1.5 IPOTESI DI RESPONSABILITA' PENALE

Non si può, in questa sede esaminare tutti i reati che possa commettere il certificatore: come si è avuto modo di esporre ampiamente in precedenza il tipo di responsabilità penale sarà determinata dalla soluzione del problema sulla natura dell'attività di costoro, da cui peraltro scaturiscono diverse responsabilità per l'utente.

Qualora, come è opinione di chi scrive, si voglia rivestire il certificatore della pubblica fede entrerebbero in gioco, tra gli altri, reati gravi sulle falsità.

Si pensi ad esempio al caso in cui il certifcatore, nell'espletare la sua attività, proceda alla creazione di un certificato in cui riporta intenzionalmente contenuti non veritieri.

Laddove lo si ritenga un pubblico ufficiale, egli potrà essere chiamato a rispondere, ricorrendone i requisiti oggettivi e soggettivi, del reato di cui all'art.480 c.p., *"Falsità ideologica commessa da pubblico ufficiale in certificati o in autorizzazioni amministrative"*

Oppure accedendo alla stessa concezione, e allorquando la falsità sia materiale e non ideologica, potrà trovare applicazione l'art. 477 c.p.,

“Falsità materiale commessa da pubblico ufficiale in certificati o in autorizzazioni amministrative”

Per ben comprendere cosa comporti una qualificazione, piuttosto che un'altra del certificatore, si tenga presente che le stesse ipotesi delittuose laddove siano commesse dal privato cittadino comportano un trattamento sanzionatorio decisamente più tenue.

Al di là dell'esempio sopra riportato la qualificazione o qualificabilità del certificatore come pubblico ufficiale apre scenari nuovi ed interessanti, senza dubbio meritevoli di un analitico approfondimento nelle opportune sedi di dibattito e di confronto.

Si pensi ad esempio all'applicabilità al certificatore delle disposizioni relative ai delitti dei pubblici ufficiali contro la pubblica amministrazione: è irrealistico immaginare che il certificatore possa essere chiamato a rispondere per concussione? O per corruzione per un atto d'ufficio? O contrario ai doveri d'ufficio?

A parere di chi scrive la risposta non può che essere negativa: e tuttavia proprio per la gravità delle implicazioni che una simile opzione ermeneutica comporta, si reputa altresì necessario un intervento del legislatore in grado di chiarire i dubbi che l'attuale normativa può generare.

Dubbi che quando investono la sfera penale risultano assai più odiosi perchè inevitabilmente confliggenti con la libertà dell'individuo, bene supremo ed insopprimibile in uno stato di diritto.

BIBLIOGRAFIA

Antolisei F., *Manuale di diritto penale, parte speciale II*, 1997, Giuffrè

Borruso R., Di Giorgi R.M., Mattioli L., Ragona M., *L'informatica del diritto*, 2004, Giuffrè

Borruso R., Tiberi C., *L'informatica per il giurista*, 2001, Giuffrè

Buonomo G., *La responsabilità del certificatore nel sistema di firma digitale*, pubblicato il 3 ottobre 2002, www.interlex.it

Cammarata M., Maccarone E., *La firma digitale sicura*, 2003, Giuffrè

Iaselli M, *Informatica Giuridica*, 2002, Edizioni Simone

Miccoli, *Documento e commercio telematico*, IPSOA 1998

Neirotti L., *Aspetti giurdici della sicurezza della firma elettronica e delle smart cards*, in *Ciberspazio e Diritto*, n. 3-4/2003

Parodi C., Calice A., *Responsabilità penali e Internet*, IL SOLE 24 ORE, pp. 163 ss.

Sarzana di S. Ippolito, *Documento informatico, firma digitale e crittografia. Riflesioni giuridiche e penalistiche, in* Atti convegno ITA " *La firma elettronica e le regole tecniche*", Roma 15 – 16 luglio 1999, pp 7 ss.