GUIDA PRATICA SU FIRME ELETTRONICHE
E FIRME GRAFOMETRICHE

A cura del Digital & Law Department – Studio Legale Lisi

Aggiornata alle nuove regole tecniche definite con DPCM 22 febbraio 2013

INDICE

Autori della Guida:
Avv. Andrea Lisi
Avv. Luigi Foglia
Avv. Graziano Garrisi
Avv. Sarah Ungaro

Introduzione a cura del *Notaio Avv. Eugenio Stucchi*

Testo aggiornato al 20/05/2014

PREFAZIONE

Negli ultimi anni si sente sempre più spesso parlare di documento informatico e di firme elettroniche ma, nonostante l'Italia sia stata il primo stato europeo a disciplinare una propria firma elettronica (la firma digitale), questi strumenti stentano ancora a essere diffusi e correttamente utilizzati.

La firma digitale, in particolare, presenta ancora qualche difficoltà di utilizzo dovuta, in gran parte, a una scarsa conoscenza da parte del firmatario delle corrette modalità di utilizzo dello strumento di firma, ma anche a una normativa che, ancora oggi, lascia qualche zona d'ombra esponendo il fianco ai detrattori dell'innovazione digitale.

Accanto alla firma digitale si sta affacciando sul mercato la firma elettronica avanzata (FEA) al momento ancora in attesa di una regolamentazione compiuta da parte del nostro legislatore. In questo insieme indefinito di soluzioni tecnologiche (o meglio ancora di “processi”) in grado di legare un documento a un individuo, si stanno facendo conoscere sempre di più sul mercato le firme grafometriche.

Basandosi sul comportamento tenuto da una persona nell'atto di firmare, le firme grafometriche promettono di riuscire a legare un documento al sottoscrittore mediante un'operazione che esternamente è quasi identica alla classica firma sul foglio di carta, ma che nasconde in realtà avanzati processi di riconoscimento biometrico.

Le soluzioni prospettate dai vari “vendor” differiscono molto tra loro; presentano, ognuna, peculiarità e specifiche tecniche spesso taciute ai meno accorti.

Come districarsi in questo nuovo mondo della sottoscrizione elettronica? Quali sono i profili legali da tenere in considerazione e quali i relativi rischi?

E i nostri dati biometrici, quali rischi corrono? Come devono essere trattati?

La presente Guida fornisce risposte concrete, a queste e ad altre domande, utili a chi voglia orientarsi in questo nuovo e stimolante settore.

INTRODUZIONE

Non è inutile riflettere un istante sul titolo della piccola guida che abbiamo tra le mani, o meglio più impalpabilmente davanti agli occhi. Essa è intitolata "Guida pratica su firme elettroniche e firme grafometriche". Emendando i tecnicismi, è evidente che ci accingiamo a leggere una guida che si propone nella sostanza di spiegare al lettore "come firmare", e come far firmare.

Da secoli e millenni l'uomo produce documenti, passando dai supporti più vari, dalla pietra alla cera, dal papiro alla pergamena, alla carta e forse mai prima d'ora si era sentita la necessità di scrivere una vera e propria guida che spiegasse l'atto del "come firmare", che spiegasse come firmare in modo sicuro, che districasse i concetti tra oltre quattro distinti tipi di firme, con effetti giuridici in parte diversi.

Scrivere il proprio nome e cognome in chiaro è stato per millenni forse il primo gesto di calligrafia insegnato, che metteva immediatamente il soggetto in grado di poter sottoscrivere qualsiasi tipo di documento, senza eccessive ulteriori spiegazioni, e con efficacia giuridica intuitiva. Mettere nero su bianco, vincolare in modo serio.

Certo dobbiamo riconoscere che siamo davanti alla più grande rivoluzione culturale e giuridica da millenni, che vede per la prima volta il documento svincolato dal proprio supporto, la pietra, la tavoletta di cera, la pergamena o il nostro foglio di carta vengono polverizzati e trasformati in una serie di numeri in ultima analisi binari; rivoluzione che non può che comportare una certa complicazione, non fosse altro perché in fondo noi siamo esseri umani con organi di senso analogici, che quindi non digeriscono facilmente grosse moli di numeri, che pertanto per essere resi a noi conoscibili debbono necessariamente essere riconvertiti in stimoli analogici. Se prima quindi si era sicuri che apponendo la propria firma su un determinato documento si stava firmando proprio quello, ora si aprono abissi tecnici e filosofici, perché intervenire su una polvere di numeri non è altrettanto intuitivo come vergare il proprio nome e cognome su uno spesso foglio forse ingiallito, ma saldamente nelle nostre mani, e non sapremo mai più con la stessa certezza che quello che firmiamo è proprio quello che stiamo leggendo.

Siamo di fronte quindi a una ineliminabile complicazione, compensata, riteniamo, da una più agile, rapida ed economica gestione del documento. Dovremmo però interrogarci se forse non si è andati troppo oltre. Se forse la disciplina delle firme elettroniche non sia davvero troppo travagliata, come indicato più innanzi nella guida. Se forse seguire i link www.aipa.it, e poi di rimando www.cnipa.it, e poi ancora di rimando www.digitpa.it - con un incremento esponenziale della cacofonia - e poi ancora di rimando la nuova, costituenda "Agenzia per l'Italia Digitale", non sia specchio di un legislatore che, pur animato da ottime e lodevoli intenzioni, cercando di scendere troppo nel tecnico, viene condannato continuamente a inseguire un cambiamento troppo veloce.

Ed in questa linea di pensiero non è inutile domandarsi se forse, inaspettatamente, il nostro "vecchio" Codice Civile non ritorni attuale, con norme giuridiche che possiamo ritenere applicabili anche alle nuove tipologie di firma, a ricordarci che il compito del legislatore è quello di dettare regole primarie, di ampio respiro, svincolate dal particolare ed effimero dato tecnico, e compito dei giurisiti è quello di agire sugli altri formanti del diritto andando ad incasellare la cangiante e sempre mutevole realtà all'interno delle categorie giuridiche esistenti.

Ed in questo senso, di estremo interesse sono le riflessioni in tema di firma grafometrica che la riconducono con un'intuizione davvero notevole per la sua limpida semplicità - intesa nel senso più nobile e raro del termine - ai principi generali del nostro ordinamento e del nostro Codice Civile.

Con essa forse la sottoscrizione torna ad essere semplice, forse torna ad essere un atto manuale, istintivo, giuridicamente vincolante non a seguito di improbabili e precarie "regole tecniche" (sorta di atipica meteora giuridica) ma del nostro ordinamento giuridico, nel suo substrato più profondo.

Certo, anch'essa richiede particolari e importanti accorgimenti tecnici per essere gestita con sicurezza, perché dobbiamo ricordare che se in passato chi ci rubava un foglio, magari anche sottoscritto, poteva forse riempirlo a piacimento, con effetti sì gravi, ma limitati, ora chi ci rubasse una firma grafometrica, che in quanto semplice algoritmo di numeri è infinitamente riproducibile, è come se ci rubasse non un foglio, ma la nostra mano, con effetti gravissimi e potenzialmente illimitati. E in questo senso appare giusto se non indispensabile che le chiavi di cifratura dei dati grafometrici non siano nella disponibilità di alcuna delle parti contraenti, soprattutto laddove una delle parti sia soggetto forte o dominante, ma vengano custodite da soggetti terzi ed indipendenti.

La guida che abbiamo davanti agli occhi, quindi, con lodevole sforzo tira le fila della complessa normativa europea e italiana, ponendosi come autorevole supporto all'attività di operatori, professionisti e studiosi, e allo stesso tempo lancia un'intuizione che forse rappresenta la vera luce da seguire, per rendere davvero semplice il documento del futuro.

Notaio Eugenio Stucchi
www.notaipiniestucchi.it

1. Le firme elettroniche

1.1 Il documento elettronico e le tipologie di firma

Il documento informatico è la "rappresentazione informatica di atti, fatti, dati giuridicamente rilevanti"[1].
Quest'ampia definizione fa sì che vengano compresi in questa nozione elementi di vario genere: da un filmato digitale a un tracciato EDI, dai log file generati da una transazione commerciale su un sito web a una comunicazione e-mail. Tali documenti però, al contrario di quelli cartacei, sono più facilmente soggetti a modifiche e duplicazioni che pongono il necessario problema della loro sopravvivenza nel tempo e della loro validità giuridica[2].
In merito a tale profilo, ai sensi dell'art. 20, comma 1 *bis*, del Codice dell'amministrazione digitale (D.Lgs. n. 82/2005, di seguito CAD), il documento informatico soddisfa i requisiti della forma scritta quando garantisce in modo oggettivo qualità, integrità, sicurezza e immodificabilità: in base alle medesime caratteristiche, il documento informatico fornito di firma elettronica "semplice" è, inoltre, liberamente valutabile in giudizio, secondo l'art. 21, comma 1, del citato Codice.
Già da una prima analisi delle norme, viene dunque in rilievo l'importanza assunta dalle tecnologie scelte per salvaguardare il documento informatico e, tra queste, rientra sicuramente la firma elettronica.
Infatti, se nel mondo analogico utilizziamo il documento scritto e sottoscritto per avere una documentazione certa che mantenga traccia delle nostre azioni e possa essere utilizzata ed esibita in caso di contestazione, per ottenere le medesime garanzie nel mondo digitale dobbiamo utilizzare dei processi informatici che possano parimenti garantire la paternità di un documento e preservarne l'integrità/autenticità.
A tale scopo abbiamo nel nostro ordinamento quattro tipologie di firma elettronica (previste dall'art. 1 del CAD):

- FIRMA ELETTRONICA SEMPLICE (lett. q) - *L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*;
- FIRMA ELETTRONICA AVANZATA (lett. q-bis) - *Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati*;
- FIRMA ELETTRONICA QUALIFICATA (lett. r) - *Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma*;
- FIRMA DIGITALE (lett. s) - *Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica,*

[1] Art. 1, comma 1°, lett. p) del Codice dell'amministrazione digitale, di cui al D.Lgs. n. 82/2005, come modificato dal D.Lgs. 235/2010.

[2] A. Lisi, *Le nuove frontiere del documento informatico e della firma elettronica: dalla firma digitale attraverso quella grafometrica fino alla "mobile signature"*, 2012

rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

La firma elettronica semplice, strumento concepito a livello comunitario soprattutto per regolamentare le transazioni commerciali tipiche dell'*e-commerce* (dal pagamento effettuato *on line* mediante una carta di credito, sino a quello eseguito tramite uno *smart-phone*[3]), può essere idonea a far acquistare al documento informatico su cui è apposta il valore di forma scritta in base alle caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità del processo attraverso il quale si è formata: spetta, infatti, al giudice di volta in volta esprimere un giudizio sul valore probatorio di un documento sottoscritto con una firma elettronica semplice.

Alle altre tre tipologie di firma, invece, viene riconosciuta la medesima validità della "forma scritta e sottoscritta" anche se con notevoli limitazioni per la firma elettronica avanzata (FEA)[4].

1.2 La travagliata storia delle firme elettroniche in Italia

La prima normativa a livello europeo sulle firme elettroniche fu emanata con la Direttiva 1999/93/CE, attraverso la quale furono introdotti i concetti di firma elettronica c.d. semplice e firma elettronica avanzata.

Purtroppo, tale definizione di firma elettronica avanzata, così come contemplata dal Legislatore europeo, mal si attagliava alla nostra firma digitale, già definita nel D.P.R. n. 513/1997.

Perciò, dopo un primo formale recepimento della Direttiva (con il D. Lgs. n° 10/2002) nei termini in cui era stata emanata, nel 2003 in Italia sono stati disciplinati due ulteriori tipi di firma elettronica rispetto a quelli indicati dalle norme comunitarie, ossia quella qualificata e nuovamente quella digitale (D.P.R. n. 137/2003).

Inoltre nel 2005, con l'approvazione del Codice dell'Amministrazione digitale (D.lgs. n. 82/2005), il legislatore italiano ha inteso nuovamente ribadire la particolare valenza della firma digitale, a scapito delle firme elettroniche avanzate e diversamente da quanto disposto dalla citata direttiva comunitaria. In tal modo, dalle 4 tipologie di firma elettronica del 2003 si è passati alle 3 della normativa del 2005, perdendo, però, proprio la nozione di firma elettronica avanzata menzionata nella Direttiva europea dell'ormai lontano 1999.

All'estromissione della firma elettronica avanzata dall'ordinamento italiano si è assistito fino al 2010, quando il nostro Legislatore da un lato ha riconosciuto l'avanzamento tecnologico in quello specifico settore e, dall'altro, ha inteso uniformarsi a quanto dettato dalle norme comunitarie in tema di firme elettroniche.

Occorre evidenziare, tuttavia, che il ritorno in auge delle firme elettroniche avanzate ha condotto a degli eccessi paradossali: infatti, con le modifiche al CAD intervenute con il D.lgs. n. 235/2010 si è giunti al punto di parificare formalmente la firma elettronica avanzata a quella digitale, poiché entrambe risultano avere lo stesso valore giuridico e probatorio, ovvero quello previsto per le scritture private dal nostro codice civile, senza dare al contempo opportuno risalto ai differenti livelli di garanzia sulla provenienza e l'integrità offerti dai due sistemi di firma.

---

[3] Ci riferiamo alla tecnologia RFID-NFC presente nei dispositivi cellulari di ultima generazione e supportata dalle più conosciute piattaforme mondiali di carte di credito-debito.

[4] Cfr. A. Lisi, cit.

Certo, anche nella disciplina del CAD qualche differenza rimane. Alla firma digitale sono comunque riconosciute superiori caratteristiche di sicurezza e per questo, in alcuni casi, è richiesta obbligatoriamente per fornire maggiori garanzie.

Infatti, se la firma digitale (insieme alle firme elettroniche qualificate) è affidabile *in re ipsa* e garantisce con certezza al documento informatico su cui è apposta imputabilità giuridica e forma scritta grazie alla presenza di rigorosi standard internazionali che ne regolamentano tecnologie e processi di realizzazione, la firma elettronica semplice e la firma elettronica avanzata non hanno, al contrario, dei riferimenti tecnologici univoci e chiaramente delineati: per questo motivo la loro affidabilità è direttamente conseguente al contesto in cui vengono utilizzate e alle soluzioni tecnologiche a cui si ricorre.

Le firme elettroniche avanzate, dunque, nel 2010 sono state reinserite nel nostro ordinamento ma, a parte una scarna definizione formale, è mancata, fino al 2013, una loro sostanziale regolamentazione che è arrivata solo con la pubblicazione in Gazzetta Ufficiale, Serie Generale n.117 del 21-5-2013, del DPCM 22 febbraio 2013 recante *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71.*

1.3 La firma digitale

Nell'attuale formulazione, il Codice dell'Amministrazione digitale definisce la firma digitale come *species* del più ampio *genus* delle firme elettroniche avanzate, diversamente dalla disposizione previgente che la riconduceva al novero delle firme elettroniche qualificate e contemplava il riferimento al dispositivo sicuro di firma, omesso invece nella nuova definizione.

Con specifico riferimento al suo valore probatorio, il documento informatico dotato di firma digitale soddisfa pienamente il requisito della forma scritta anche quando questa è richiesta a pena di nullità, come nelle ipotesi previste dai numeri da 1 a 12 dell'art. 1350 c.c. Il documento su cui è apposta una firma digitale, inoltre, fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto, se colui contro il quale il documento è prodotto ne riconosce la sottoscrizione, ovvero se questo è legalmente considerato come riconosciuto (art. 2702 codice civile).

In ogni caso, il documento firmato digitalmente si presume riconducibile al titolare del dispositivo di firma, a meno che quest'ultimo non fornisca prova contraria (sulla scorta di quanto previsto dall'art. 21, comma 2, del Codice dell'amministrazione digitale): ciò in virtù del fatto che il sistema di verifica della firma si basa comunque su un metodo sicuro, qual è quello delle doppie chiavi asimmetriche.

Tale sistema è fondato sull'uso di due chiavi diverse, una diretta per cifrare e una inversa per decifrare (ciò comporta che non è possibile decifrare il testo con la stessa chiave usata per cifrarlo), generate insieme nel corso di un unico procedimento e correlate univocamente: una delle due chiavi può essere resa pubblica (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), mentre l'altra deve essere mantenuta segreta. Pur conoscendo una delle due chiavi, infatti, non c'è nessun modo di ricostruire l'altra.

Inoltre, per evitare di cifrare e decifrare l'intero documento si ricorre a una semplificazione che consiste nel cifrare solo un brevissimo riassunto del documento stesso, ottenuto con una procedura detta funzione di *hash*: tale funzione restituisce una stringa di caratteri che costituisce l'impronta del testo (*digest*).

Infatti, 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, è certo che esso provenga da chi appare come il titolare della chiave pubblica e che il documento non è stato alterato dopo la generazione della firma digitale.

La pubblicazione e il controllo delle chiavi avvengono accedendo ad appositi registri, ovviamente per via telematica, che devono essere correttamente tenuti e aggiornati da una terza parte fidata, generalmente nota come *Certification Authority* o certificatore, che ha il compito di gestire il *database* delle chiavi pubbliche e dei relativi certificati delle chiavi, nonché la responsabilità di procedere alla previa identificazione del soggetto che richiede la certificazione.

L'insieme degli elementi che compongono tale processo si definisce "infrastruttura di chiave pubblica" (*Public Key Infrastructure*, PKI), che si articola nei soggetti che vi partecipano (utente, certificatore, destinatario), nelle modalità in cui ciascuno di essi assolve al proprio ruolo e nelle forme di utilizzazione delle tecnologie disponibili.

Per quanto riguarda l'utilizzo in concreto di un sistema di firma digitale, l'operazione di firma in sé non costituisce un'azione di particolare complessità. Tuttavia, nei casi in cui si renda necessaria la firma di molteplici documenti, è possibile ricorrere alle procedure automatiche di firma, che rendono più rapido il meccanismo di apposizione della firma digitale.

1.4 Le firme automatiche e le firme da remoto

Le procedure automatiche di firma sono disciplinate dall'art. 35 del CAD e dal DPCM 30 marzo 2009, che ne specificano anche alcuni requisiti e impongono la garanzia di determinati livelli di sicurezza.
Il comma 3 dell'art. 35 del CAD stabilisce, infatti, che la firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima, poiché non si applica la disposizione di cui al secondo periodo del comma 2 dello stesso articolo, in base alla quale i documenti informatici devono essere presentati al titolare prima dell'apposizione della firma e occorre obbligatoriamente richiedere allo stesso la conferma della volontà di generare la firma.
Il nuovo DPCM 22 febbraio 2013, diversamente dalle precedenti regole tecniche, fornisce una definizione precisa di firma automatica quale *particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo* (art. 1 lett. r).
Sempre in tema di firme realizzate con procedure automatiche, le nuove regole tecniche, ai commi 2 e 3 dell'art. 5, prevedono che la coppia di chiavi utilizzata sia destinata esclusivamente a tale scopo (con espressa indicazione nel certificato) e sia diversa da tutte le altre coppie di chiavi in possesso del titolare. Inoltre, se tale procedura fa uso di un insieme di dispositivi sicuri per la generazione della firma elettronica qualificata o firma digitale del medesimo soggetto, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo utilizzato dalla procedura automatica.
Con particolare riferimento all'effettivo funzionamento delle firme automatiche, occorre precisare che queste non vengono realizzate mediante l'utilizzo dei comuni dispositivi forniti dai certificatori (*token usb* o *smart card*), ma si ricorre a strumenti tecnologicamente più avanzati e in grado di gestire più velocemente una maggiore quantità di dati. Al fine di garantire i livelli di sicurezza individuati dall'art. 35

del CAD, solitamente si ricorre all'utilizzo di sistemi particolarmente sicuri quali gli HSM (*Hardware Security Module* - insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in sicurezza una o più coppie di chiavi crittografiche).

Per quanto riguarda, invece, le firme da remoto (*server side*), queste costituiscono una tipologia di firma elettronica avanzata o di firma digitale utilizzabile via web: la chiave privata del firmatario e il relativo certificato di firma vengono conservati da parte di un certificatore accreditato in un server remoto basato su un sistema HSM.

Nell'attuale disciplina delle firme digitali da remoto, sia il CAD sia le attuali regole tecniche contenute nel DPCM 22 febbraio 2013[5] non vietano che i certificati possano essere generati su di un dispositivo remoto non posseduto direttamente dal titolare (come avviene mediante l'utilizzo di strumenti quali, ad esempio, la *smart card* o un *token usb*), ma impongono che il Titolare mantenga in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma.

Le nuove regole tecniche prevedono che la firma remota possa essere generata solo su HSM custodito e gestito, sotto la loro responsabilità, dal certificatore accreditato ovvero dall'organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi ovvero dall'organizzazione che richiede al certificatore di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi.

Il certificatore dovrà sempre essere in grado, dato un certificato qualificato, di individuare agevolmente il dispositivo afferente la corrispondente chiave privata.

Inoltre, nel caso in cui l'HSM non sia sotto la custodia diretta del certificatore, quest'ultimo dovrà:

a) indicare al soggetto che custodisce il dispositivo le procedure operative, gestionali e le misure di sicurezza fisica e logica che tale soggetto è obbligato ad applicare;

b) effettuare verifiche periodiche sulla corretta applicazione delle indicazioni di cui alla lettera a), che il soggetto che custodisce il dispositivo ha l'obbligo di consentire e agevolare;

c) redigere i verbali dell'attività di verifica che potranno essere richiesti in copia dall'Agenzia per l'Italia Digitale ai fini dell'attività di vigilanza prevista all'art. 31 del CAD;

d) comunicare all'AgID il luogo in cui i medesimi dispositivi sono custoditi;

e) effettuare ulteriori verifiche su richiesta dell'AgID consentendo la partecipazione anche a incaricati dello stesso ente;

f) assicurare che il soggetto che custodisce il dispositivo si impegni a consentire le verifiche sia da parte del certificatore che dell'AgID.

Il certificatore, inoltre, nel caso in cui venga a conoscenza dell'inosservanza di quanto previsto dalle regole tecniche, dovrà procedere alla revoca dei certificati afferenti alle chiavi private custodite sui dispositivi oggetto dell'inadempienza.

Sempre le nuove regole tecniche, al comma 7 dell'art. 3, richiedono che ogni procedura di firma remota sia realizzata con misure tecniche e organizzative, esplicitamente approvate per le rispettive competenze, da AgID, nell'ambito delle attività di cui agli articoli 29 e 31 del CAD, e da OCSI, per quanto concerne la

[5] L'art. 1 lett. q) del DPCM 22 febbraio 2013 definisce la firma remota come: *particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.*

sicurezza del dispositivo ai sensi dell'art. 35 del Codice, e tali da garantire al titolare il controllo esclusivo della chiave privata.
Come ogni altro dispositivo sicuro di firma, infatti, anche un HSM, ai sensi del richiamato art. 35 del CAD, dovrà garantire determinati livelli di sicurezza. A tal fine, il CAD assegna all'Organismo di Certificazione della Sicurezza Informatica (OCSI) il compito di accertare, sulla base di uno specifico schema di valutazione, la rispondenza dei sistemi di generazione delle firme ai requisiti e alle specifiche prescritte dall'allegato 3 della Direttiva 1999/93/CE e agli ulteriori requisiti stabiliti dalle regole tecniche in materia di firme elettroniche.
In base a queste considerazioni, prima di utilizzare un sistema HSM è necessario assicurarsi che quest'ultimo abbia ottenuto la necessaria certificazione presso l'OCSI[6] richiesta dall'attuale normativa.

1.5 Le firme elettroniche avanzate: le nuove regole tecniche

In questo contesto si inseriscono le nuove soluzioni di firma elettronica avanzata (FEA) che, dopo le modifiche introdotte dal D.lgs. n. 235/2010 al Codice dell'Amministrazione Digitale, sono riapparse prepotentemente sul mercato.

La normativa primaria disciplina solo i requisiti fondamentali di tali tipologie di firma, presenti nella relativa definizione di cui all'art. 1, comma, lett. q *bis*) del CAD. Una firma elettronica avanzata, infatti, è quell'*insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.*

La regolamentazione di dettaglio delle FEA è, invece, contenuta nelle regole tecniche approvate con DPCM 22 febbraio 2013.

Le principali novità delle nuove regole tecniche attengono all'assoluta libertà tecnologica lasciata agli sviluppatori di soluzioni di firma elettronica avanzata e all'assenza di qualsiasi controllo preventivo da parte della preposta autorità di vigilanza (dunque i soggetti che erogano sistemi di firma elettronica avanzata non sono soggetti ad alcuna registrazione).

In tal modo, si è inteso liberalizzare le tipologie di firma avanzata, non vincolandole più ad un certificato qualificato o ad un dispositivo sicuro, come invece richiesto per le firme elettroniche qualificate e per quelle digitali, entrambe *species* del genere firma elettronica avanzata[7]. Ciò in quanto le firme elettroniche avanzate avranno un valore limitato al solo contesto in cui vengono utilizzate (tra il sottoscrittore e il soggetto che offre il servizio di firma)[8], rendendo quindi necessario che le loro condizioni

---

6 Sul sito dell'OCSI è possibile verificare quali HSM siano stati certificati e quali siano in corso di accertamento http://www.ocsi.isticom.it/index.php/dispositivi-di-firma .

7 Sul punto, si veda B. Santacroce, *Dalla firma digitale alla firma biometrica: quadro giuridico di riferimento per l'applicazione dei nuovi dispositivi di firma*, Minigrafia nr. 9 Il nuovo CAD. Commenti e prospettive. Atti del Convegno dell'8 luglio 2011. Roma, Accademia dei Lincei, edito dalla Fondazione Siav Academy.

8 Ai sensi dell'art. 60 del DPCM 22 febbraio 2013 relativo alle Regole tecniche sulle firme elettroniche.

di utilizzo siano preventivamente accettate per iscritto dagli utenti[9]. Per questi motivi, il soggetto che realizza la soluzione di firma elettronica avanzata dovrà informare gli utenti in merito agli esatti termini e condizioni relativi al servizio, compresa ogni eventuale limitazione dell'uso.

Le soluzioni di firma elettronica avanzata non sono costituite da un determinato software, né da una determinata tecnologia, ma rappresentano un sistema neutro, sicuro e affidabile idoneo a garantire la riconducibilità di un documento informatico, reso immodificabile, al soggetto che l'ha sottoscritto.

A tal fine, queste devono assicurare:

a) l'identificazione del firmatario del documento;

b) la connessione univoca della firma al firmatario;

c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima;

d) la possibilità di verificare che il documento informatico sottoscritto non abbia subìto modifiche dopo l'apposizione della firma;

e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;

f) l'individuazione del soggetto di cui all'articolo 55, comma 2, lettera a);

g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;

h) la connessione univoca della firma al documento sottoscritto[10].
Qualora i sistemi di firma elettronica in concreto adottati non dovessero assicurare i requisiti innanzi richiamati (ad eccezione della lett. f)) la firma elettronica generata non potrà soddisfare le caratteristiche previste dagli articoli 20, comma 1 *bis*, e 21, comma 2, del CAD, ossia qualità, sicurezza, integrità ed immodificabilità.

In generale, dall'art. 57 delle Regole tecniche si evince che in capo ai soggetti che realizzano soluzioni di firma elettronica avanzata è posto l'obbligo di identificare in modo certo l'utente tramite un valido documento di riconoscimento, di informarlo circa gli esatti termini e condizioni relativi al servizio, compresa ogni eventuale limitazione dell'uso, di subordinare l'attivazione del servizio stesso alla previa sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente, conservando copia dei documenti di riconoscimento e della dichiarazione di accettazione delle condizioni d'uso relativi a ogni utente per almeno venti anni.

---

[9] All'art. 57 delle Regole tecniche sulle firme elettroniche viene contestualmente contemplata una deroga in ambito sanitario, in quanto si stabilisce che la dichiarazione di accettazione delle condizioni del servizio da parte dell'utente possa essere effettuata anche oralmente, con le modalità previste per la prestazione del consenso di cui all'art. 81 del D.Lgs. 30 giugno 2003, n. 196.

[10] Art. 56, co. 1, del DPCM 22 febbraio 2013 (Regole tecniche sulle firme elettroniche).

In ogni caso, occorre tenere presente che tutto il processo relativo alla firma elettronica avanzata deve essere orientato alla sicurezza delle informazioni trattate; inoltre, devono anche essere garantite l'integrità e la leggibilità dei dati e deve anche essere impedito ogni possibile accesso abusivo ai dati stessi (soprattutto quando i dati trattati siano di tipo biometrico). A tal fine, si consiglia l'adozione di standard internazionali relativi alla sicurezza delle informazioni trattate (ISO 27001)[11].

Inoltre, è di estrema importanza che tutte le fasi del processo siano correttamente registrate e che i relativi *log file* siano conservati insieme ai documenti e a tutte le altre informazioni relative al processo di firma elettronica.

Un idoneo sistema di conservazione, infatti, è in grado di garantire l'integrità dei dati oggetto di archiviazione e consentirà l'esibizione dei documenti e delle relative informazioni ad essi associate (informazioni che unitamente al documento di riconoscimento costituiscono la FEA).

[11] L'art. 58 del DPCM 22 febbraio 2013 richiede alcune certificazioni obbligatorie per le soluzione di firma elettronica avanzata realizzate da privati in favore di amministrazioni pubbliche (ISO/IEC 27001 e ISO 9001).

2. La firma grafometrica

2.1 La firma biometrica e la firma grafometrica

Con la locuzione “autenticazione biometrica” si fa riferimento all’identificazione o alla verifica automatica dell’identità attraverso strumenti di valutazione di caratteristiche fisiche o comportamentali (Linee Guida CNIPA 2004). Con questa definizione, sin dal 2004, l’ordinamento italiano ha preso in considerazione l'utilizzo di dati biometrici per la corretta identificazione personale.

Tutti i sistemi biometrici sono caratterizzati da un processo che consiste nel confronto tra dati fisici o comportamentali propri di un determinato soggetto con un campione degli stessi dati precedentemente acquisiti: l’intero processo inizia con una fase di registrazione dei dati biometrici per mezzo di un dispositivo di acquisizione, i quali vengono elaborati per estrapolarne il c.d. *template*, ossia una rappresentazione matematica dei dati biometrici stessi.
Questa sequenza di numeri che rappresenta i dati biometrici acquisiti viene poi registrata in un *database* o su una *smartcard*.
In seguito, durante tutti i successivi processi di verifica, vengono nuovamente acquisiti i dati biometrici e ricavata la relativa stringa numerica, la quale viene confrontata con quella precedentemente ottenuta in fase di registrazione.
Oltre che per la corretta identificazione, il *template* così formato può essere utilizzato come “dato per la creazione della firma” (si veda la Direttiva 1999/93/CE), al fine di soddisfare tutti i requisiti necessari per una firma elettronica avanzata, cifrando, ad esempio, l’impronta del documento mediante l’utilizzo dello stesso *template* biometrico.
Tra le varie firme che è possibile ottenere utilizzando dati biometrici, particolare attenzione meritano le firme grafometriche. Tali firme, infatti, realizzate mediante la memorizzazione dei dati comportamentali dell’utente legati all’apposizione materiale della firma hanno l'indubbio vantaggio di rendere possibile un'implementazione elettronica della sottoscrizione di un documento, permettendo allo stesso utente di firmare nello stesso modo in cui ha sempre fatto sulla carta.
Sul punto è innanzitutto opportuno sgombrare il campo da possibili confusioni distinguendo le firme grafometriche dalle firme realizzate con prodotti hardware che si limitano ad acquisire l’immagine digitale della firma del sottoscrivente attraverso un *tablet*, poiché in tale procedimento non viene acquisito alcun dato biometrico. Per tale motivo, questo tipo di firma può essere facilmente disconosciuta, in quanto rimane priva degli ulteriori elementi grafometrici tipici della “sottoscrizione su carta” e non possiede, quindi, elementi concretamente utilizzabili in un processo di verifica: la sua efficacia giuridica rimane dunque quella prevista dagli artt. 2712[12] e 2719[13] del Codice Civile.
Nei sistemi in cui, invece, l’acquisizione di dati dal *tablet* non si limiti alla mera immagine della firma, ma riguardi anche i dati grafometrici che caratterizzano il comportamento del sottoscrivente (parametri quali la velocità di scrittura, la pressione esercitata, l’angolo d’inclinazione della penna, l’accelerazione del

[12] Art. 2712 (Riproduzioni meccaniche) *Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.*

[13] Art. 2719 (Copie fotografiche di scrittura) *Le copie fotografiche di scritture hanno la stessa efficacia delle autentiche, se la loro conformità con l'originale è attestata da pubblico ufficiale competente ovvero non è espressamente disconosciuta.*

movimento, il numero di volte che la penna viene sollevata dalla carta), tale processo di firma grafometrica può essere utilizzato sia come modello di sottoscrizione digitale, assicurando in questo modo un accesso in remoto al proprio certificato di firma (custodito ad esempio in un HSM[14]), sia come credenziale forte di autenticazione[15] per garantire un accesso riservato di transazione.

L'utilizzo della firma grafometrica come modello di sottoscrizione digitale, che consente un accesso in remoto al relativo certificato, rende però indispensabile la creazione di una banca dati delle firme biometriche che ne permetta il relativo riscontro, con le conseguenti ripercussioni in tema di privacy e trattamento dei dati[16] che approfondiremo più avanti.

La firma biometrica grafometrica, pur in assenza di un certificato di firma digitale, può anche essere ricompresa nel più ampio novero delle firme elettroniche avanzate (FEA) nelle ipotesi in cui sia caratterizzata da determinati requisiti, quali: l'identificazione certa del firmatario, il legame indissolubile tra firma e documento informatico sottoscritto, la garanzia dell'integrità del connubio composto dal documento e dal dato biometrico della firma.

In questi casi sarà dunque necessario implementare un vero e proprio processo informatico in grado di soddisfare detti requisiti previsti dal CAD e, in particolare, dalle Regole tecniche. Ovviamente, anche nei processi che adottano tale configurazione della firma grafometrica si richiede la creazione di un database biometrico al fine di garantire l'identificazione certa del firmatario, con i relativi profili privacy e di corretto trattamento dei dati che vengono in rilievo[17].

2.2 La firma autografa elettronica

Accanto alle tipologie di firma già analizzate, è possibile considerare anche una particolare modalità di firma grafometrica come tipologia di firma a sé stante, per la quale già esiste un riconoscimento nel nostro codice civile: in presenza di determinati presupposti, essa, infatti, ben può essere considerata una firma autografa riversata non su un foglio di carta, ma associata indissolubilmente a un documento informatico, a patto che quest'ultimo abbia i requisiti tipici previsti per garantire la forma scritta ai sensi dei già citati artt. 20 e 21 del CAD[18].

La firma autografa, scritta di proprio pugno, in fondo, non è stata sempre e solo legata alla carta. Nel tempo, varie tecnologie e supporti analogici sono stati utilizzati per acquisire e conservare i segni distintivi di ogni individuo: lo scalpello e la pietra per lo scultore, il pennello e la tela per il pittore, e così via. Allo stesso modo, mediante nuove tecnologie digitali di acquisizione e conservazione, è possibile

---

14 Gli HSM (*Hardware Security Module*), di cui si è innanzi detto, sono dei dispositivi sicuri per la firma digitale massiva.

15 Secondo l'allegato B) al Codice Privacy le credenziali di autenticazione possono consistere "*in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave*".

16 Qualunque trattamento di dati biometrici rende indispensabile una notificazione al Garante (ex art. 37 lett. a del Codice Privacy) e la proposizione di un interpello alla stessa Autorità Garante ai sensi dell'art. 17 del Codice Privacy.

17 Si veda la nota 18.

18 La firma grafometrica viene richiamata anche nel CAD all'art. 25 comma 2: *"l'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico"*.

rilevare e preservare nel tempo gli stessi elementi grafometrici[19] preservati sulla/dalla carta.

Questo costituisce un nuovo modo di intendere la firma grafometrica che permette di utilizzarla senza ricorrere sempre e comunque al preventivo confronto della firma apposta con quelle precedentemente raccolte e conservate in appositi database. Una firma che, opportunamente acquisita e legata al documento, al pari della sottoscrizione su carta, potrà così essere verificata, qualora venga disconosciuta in giudizio, con tecniche molto simili a quelle attualmente utilizzate dai periti grafologici.

In pratica, la firma "autografa elettronica" viene elaborata mediante l'utilizzo di una tavoletta grafica in grado di acquisire, con notevole precisione, gli elementi comportamentali legati alla firma e di trasformarli mediante apposite formule matematiche. Tali dati, immediatamente dopo la loro acquisizione, vengono cifrati (mediante l'utilizzo di una *Master Key*) e fusi con il documento informatico che si intende sottoscrivere.

Il processo di sottoscrizione[20], infine, si conclude con la memorizzazione di tutti i dati così elaborati su di un supporto in grado di preservarne la leggibilità nel tempo.

Qualora fosse necessario procedere alla verifica della firma (ad esempio a seguito di un disconoscimento della sottoscrizione avvenuto in giudizio) sarà possibile decriptare i dati biometrici e confrontarli con quelli raccolti in giudizio dal perito grafico incaricato, che effettuerà le proprie comparazioni secondo regole non dissimili a quelle utilizzate negli attuali processi di verifica di sottoscrizioni su carta.

Affinché tutto il processo possa offrire idonee garanzie per entrambe le parti (sottoscrittore e soggetto che intende avvalersi del documento sottoscritto), la chiave necessaria per decifrare correttamente i dati biometrici dovrà essere affidata ad una terza parte fidata[21] (ad esempio, un ente certificatore o un notaio) che sia in grado di garantirne la corretta custodia. Solo in pochi e ben individuati casi, la parte fidata prescelta effettuerà, in ambiente sicuro e chiuso (ad esempio su di un computer non connesso ad alcuna rete e su cui non siano presenti *malware* in grado di acquisire i dati elaborati), la decifratura dei dati biometrici e ne sorveglierà l'utilizzazione da parte del perito incaricato, curando anche che al termine delle operazioni peritali si proceda alla cancellazione sicura di tutti i dati elaborati.

Dalle considerazioni svolte dunque si evince come, a prescindere da quelle che sono le regole tecniche per le firme elettroniche avanzate, è comunque possibile reperire nel nostro ordinamento gli elementi giuridici a supporto della validità e dell'autonomia della firma autografa digitale[22] o grafometrica.

In ogni caso, l'utilizzo di tali tipologie di firma, però, non deve mai prescindere da una corretta formazione del documento informatico, un'adeguata conservazione dell'oggetto informatico (composto dal documento e dai dati della firma biometrica) e da una particolare attenzione verso le delicate questioni di sicurezza e privacy che essa, comunque, solleva.

---

19 In realtà le più avanzate tecniche grafometriche permettono di acquisire un numero superiore di informazioni e con una maggiore accuratezza di quelle normalmente rilevabili da un esperto grafologo sulla carta.

20 Per approfondire ulteriormente alcuni aspetti del processo di formazione delle firme grafometriche si consiglia la lettura dell'articolo *"Il decalogo della firma grafometrica"* di Giovanni Manca, pubblicato in Information Security n° 8 gen-feb 2012, Edisef.

21 Una terza parte fidata, ad esempio, può essere un ente certificatore che custodisca la Master Key in un HSM e sia in grado di offrire idonee garanzie di controllo sugli accessi ai propri sistemi. Data, però, la delicatezza delle informazioni grafometriche che si intende preservare è consigliabile rivolgersi ad un Notaio che abbia predisposto un idoneo processo di conservazione, preservazione ed eventuale utilizzo della Master Key e che, in considerazione anche della fede pubblica riconosciuta al suo ruolo, possa offrire idonee garanzie di sicurezza e affidabilità.

22 Un riconoscimento, seppur indiretto, dell'esistenza giuridicamente rilevante di tale tipologia di firma, lo si ha già nel CAD (art. 25) e nella recente normativa sull'atto pubblico informatico redatto da notaio (D.Lgs 110/2010) che riconoscono al pubblico ufficiale, la possibilità, così come avviene per le firme "analogiche", di autenticare le firme autografe acquisite digitalmente.

2.3 Aspetti legati al corretto trattamento dei dati personali

La normativa italiana in materia di protezione dati personali (d.lgs. 196/2003, c.d. Codice Privacy) consente il trattamento dei dati biometrici solo se vengono rispettate una serie di misure organizzative, tecniche e di sicurezza, così come regolamentate anche nel Documento di Lavoro sulla Biometria adottato in data 1° agosto 2003 dal Gruppo europeo per la tutela dei dati personali (costituito a norma dell'art. 29 della direttiva 95/46/CE), nelle due versioni delle Linee Guida in materia di trattamento di dati personali dei lavoratori privati e pubblici (del 23 novembre 2006 e del 14 giugno 2007)[23], e nel c.d. " Decalogo su corpo e privacy" (Comunicato stampa - 09 maggio 2006).

Il riconoscimento automatico degli individui, definiti dal Codice Privacy quali interessati al trattamento (art. 4, comma 1, lett. i), infatti, può avvenire tramite loro caratteristiche fisiologiche e/o comportamentali e, a seconda dei casi, tale trattamento può risultare più o meno invasivo, con la conseguente necessità di essere sottoposto a un maggior controllo da parte del Titolare a garanzia e tutela del dato.

In tema di trattamento di dati biometrici, infatti, l'Autorità Garante per la protezione dei dati personali ha sempre ispirato i suoi provvedimenti a princìpi di buon senso e prudenza: invero, possiamo affermare che sino ad oggi l'utilizzo del dato biometrico è stato consentito solo in casi molto particolari, per fungere da alternativa alle normali credenziali di autenticazione a un sistema informatico o di accesso a determinate aree sensibili.

Inoltre, nel già citato Decalogo sull'uso del corpo sono state tra l'altro individuate alcune garanzie tra cui:

1. ***Affidabilità del sistema*** *di rilevazione dei dati corporei, indicando il livello della sua accuratezza. La rigorosità dei controlli (preventivi e indubitabili negli esiti) deve tener conto anche di valutazioni di comitati tecnici indipendenti.*
2. ***Informativa chiara****, lasciando comunque la libertà di aderire o meno al sistema, salvo stringenti ragioni, indicando nella stessa informativa espressamente le tecniche alternative all'utilizzo dei dati corporei.*
3. ***Liceità*** *verificabile indubitabilmente sotto i profili di necessità, proporzionalità, finalità, correttezza, adeguatezza e qualità dei dati, previa acclarata dimostrazione dell'inefficacia di pratiche alternative che abbiano meno rischi di profilabili abusi. In particolare, qualora l'uso dei dati corporei sia permesso, deve essere comunque il più possibile circoscritto (ad esempio impronta di un dito invece di più dita).*
4. ***Deroga motivata*** *con uso controllato in speciali casistiche e non uso generalizzato o incontrollato o indifferenziato. Tale deroga motivata va periodicamente riesaminata, valutando la persistente sussistenza dei fattori che l'hanno determinata, anche alla luce del progresso scientifico.*
5. ***Delimitata memorizzazione*** *su circoscritti supporti correlati sempre disponibili per l'interessato e non centralizzazione sotto qualsiasi forma ed in particolare divieto assoluto di archivi*

[23] L'Autorità Garante definisce il dato biometrico come "*dati ricavati dalle caratteristiche fisiche o comportamentali della persona a seguito di un apposito procedimento (in parte automatizzato) e poi risultanti in un modello di riferimento. Quest'ultimo consiste in un insieme di valori numerici ricavati, attraverso funzioni matematiche, dalle caratteristiche individuali sopra indicate, preordinati all'identificazione personale attraverso opportune operazioni di confronto tra il codice numerico ricavato ad ogni accesso e quello originariamente raccolto*". Specifica, poi, che l'uso generalizzato e incontrollato di dati biometrici, specie se ricavati dalle impronte digitali, non è lecito. Nel trattare tali dati, infatti, sono necessarie elevate cautele per prevenire possibili pregiudizi a danno degli interessati, con particolare riguardo a condotte illecite che determinino l'abusiva "ricostruzione" dell'impronta, partendo dal modello di riferimento, e la sua ulteriore "utilizzazione" a loro insaputa.

centralizzati, anche se con dati cifrati. In particolare occorre attivare una funzione permanente di ricerca di soluzioni che evitino accumulazioni o unificazioni di dati.

6. ***Temporanea conservazione*** *in ordine cronologico per il necessario periodo limitato (e, come nel caso di associazione di dati biometrici con videoregistrazioni, per non oltre una settimana). Sono vietati, in particolare, le cosiddette copie di sicurezza che prolungano surrettiziamente i tempi di conservazione.*
7. ***Scrupolose misure di sicurezza*** *con sistemi inequivoci e senza rischio, promuovendo, obbligatoriamente ed inderogabilmente nel caso di uso congiunto di dati biometrici e di videosorveglianza in banca, l'interposizione di un "vigilatore dei dati" indipendente, individuato nel titolare di una funzione in posizione di indipendenza o da un soggetto indipendente (anche proceduralmente non essendo designato dall'organo amministrativo bensì dall'organo indipendente). In particolare nei casi prescritti va evitata anche la sola teorica possibilità di decifrare le informazioni acquisite senza l'intervento di tale vigilatore.*
8. ***Piena ed immediata conoscibilità dei dati biometrici da parte dell'interessato*** *e limitazioni stringenti (sino al completo divieto nel caso di uso incrociato di dati biometrici e videosorveglianza) per datore di lavoro, suoi dipendenti e collaboratori. Per le operazioni inerenti alla conoscenza, va promossa, ove necessaria, la cooperazione di un vigilatore indipendente (obbligatorio e inderogabile nel caso di uso incrociato di dati biometrici e videosorveglianza).*
9. ***Rispetto rigoroso degli obblighi*** *di verifica preliminare del Garante (art. 17 Codice Privacy) e di notifica al Garante (art. 37 Codice Privacy).*
10. ***Disattivazione automatica, immediata e certa di funzioni di smart card o altre analoghe*** *nel caso di smarrimento o di furto.*

In conformità al quadro comunitario, poi, l'utilizzo di dati biometrici, in quanto rientranti nella definizione di trattamento di dati che comportano rischi specifici per i diritti e le libertà fondamentali degli interessati, ha spesso come presupposto (oltre alla notificazione ex art. 37 d.lgs. 196/2003) anche uno specifico procedimento da instaurarsi presso l'Autorità Garante, ovvero quello della "verifica preliminare", che è volto ad appurare la liceità e la correttezza del trattamento e ad impartire al Titolare misure ed accorgimenti a garanzia degli interessati.

Non è raro riscontrare, infatti, casi di uso sproporzionato del dato biometrico rispetto alle finalità della raccolta (es. uso generalizzato di dati biometrici nei luoghi di lavoro o creazione di archivi centralizzati di dati biometrici[24]).

In ogni caso, i principali adempimenti da mettere in atto sono:

- distinguere la natura del dato biometrico (le problematiche giuridiche e di sicurezza variano, infatti, da dato biometrico a dato biometrico);

[24] Detta centralizzazione in una banca dati risulta di regola sproporzionata e non necessaria. I sistemi informativi, infatti, dovrebbero essere configurati in modo da ridurre al minimo l'utilizzazione di dati personali e da escluderne il trattamento, quando le finalità perseguite possono essere realizzate con modalità tali da permettere di identificare l'interessato solo in caso di necessità (artt. 3 e 11 del Codice). Una centralizzazione di tal genere, nell'ambito di un sistema di firme grafometriche, dovrebbe essere pertanto idoneamente giustificata e autorizzata dall'Autorità Garante.

- rendere effettivo agli interessati il diritto di informativa ex art. 13, di accesso ex art. 7 e la possibilità di utilizzo di sistemi alternativi di riconoscimento non biometrico (nella tematica che ci occupa si tratterebbe di trovare eventuali sistemi di firma alternativi[25]);
- ottenere l'attestazione di conformità dell'installatore del sistema;
- necessità della notificazione ex art. 37 del Codice;
- privilegiare sempre sistemi non centralizzati di conservazione dei dati biometrici (laddove possibile);
- implementare misure idonee (art. 31 d.lgs. 196/2003);
- verificare la necessità di incaricare strutture di controllo esterne;
- gestire in maniera compiuta i tempi di conservazione strettamente necessari;
- adottare in ogni caso misure di sicurezza stringenti.

Tutto quanto sopra indicato rientra tra gli adempimenti da effettuarsi sulla base anche di un "Privacy Impact Assessment", così come sostenuto anche dal Working Party 29 (WP 29), con cui recentemente (aprile 2012) i Garanti Privacy d'Europa (con l'Opinione 3/2012) si sono espressi indicando lo scenario futuro conseguente allo sviluppo delle tecniche biometriche e sottolineando gli aspetti e le problematiche da tenere presenti a livello comunitario per garantire la protezione dei dati personali.
Il lavoro svolto a livello europeo, pertanto, ha come proposito quello di fornire un quadro riveduto e aggiornato delle principali problematiche legate alla tutela della privacy nell'utilizzo di tali sistemi.
I problemi principali nell'utilizzo di firme grafometriche, infatti, derivano da furti d'identità digitale, utilizzo dei dati biometrici per un uso diverso dallo scopo per i quali sono stati raccolti ed eventuali violazioni di dati che potrebbero verificarsi se non dovessero essere adottate tutte le misure di sicurezza idonee e necessarie (ipotesi che potrebbe comportare anche la necessità di darne comunicazione a tutti gli interessati coinvolti e/o alle autorità competenti).
Nell'elenco delle misure e degli accorgimenti elaborati nell'Opinione del WP 29 viene fatta una differenziazione in termini di misure tecniche e misure organizzative.
Le misure tecniche di interesse per gli aspetti di firma grafometrica prevedono:

- **utilizzo di "biometric template"**, ossia informazioni chiave estratte dai dati biometrici raccolti e successivamente trattate in luogo dei dati biometrici stessi. È chiaro che questa indicazione va intesa come "laddove applicabile": per esempio nel caso di firma grafometrica i dati raccolti (pressione impressa al tratto, velocità e accelerazione della scrittura ecc.) potrebbero dare luogo al relativo "biometric template" che è l'oggetto di trattamento;
- **conservazione dei dati biometrici su dispositivi ad uso esclusivo dell'interessato**, se non risulta indispensabile utilizzare database centralizzati, prevedendo di:
  - eseguire le necessarie operazioni di confronti/lettura dei dati (crittografati) direttamente sui dispositivi in uso esclusivo dell'interessato;
  - conservare su tali dispositivi il minor numero possibile di dati identificativi dell'interessato (per limitare i rischi di furto d'identità digitale);

[25] La lett. f) del comma 1 dell'art. 57 delle Nuove regole Tecniche sulle firme elettroniche richiede ai soggetti che utilizzano per proprio conto una soluzione di FEA di consentire, accanto a questa, anche l'uso della firma digitale o di altra firma elettronica qualificata.

- mantenere sempre i dati crittografati qualora sia effettivamente necessaria la conservazione di dati biometrici in database centralizzati;

- **rinnovabilità e revocabilità**, intesa come:
  - possibilità tecnica/organizzativa di rigenerare i dati in modo sicuro a seguito di una violazione dei dati stessi o a seguito di evoluzioni tecnologiche;
  - possibilità per l'interessato di esercitare il diritto di revoca della connessione tra la sua identità e i dati biometrici elaborati;
- **crittografia** (ovvero la necessità di mantenere sempre crittografati i dati biometrici e assegnare le chiavi di decrittazione esclusivamente a coloro che hanno effettiva necessità di conoscere i dati);
- **antispoofing (**ai produttori è indicato di implementare sistemi in grado di determinare la genuinità dei dati biometrici conservati ed il loro collegamento alla persona fisica, ai fini della affidabilità dello specifico sistema biometrico).

Il WP 29 considera come meritevoli di interesse le tecniche di crittografia/decrittografia biometrica, ovvero quelle basate sull'utilizzo di dati biometrici per creare le chiavi di crittazione/decrittazione. Si tratta di metodi automatizzati per la cancellazione dei dati, poiché la cancellazione del dato, allo scadere del termine entro il quale è necessaria la sua conservazione, è considerata una delle più importanti misure nel trattamento biometrico per limitare i rischi di furti di identità ed uso improprio dei dati.

Le misure organizzative prevedono:

- **procedure interne** (ovvero stabilire chiare procedure per determinare i limiti e le modalità di accesso esclusivamente per gli aventi diritto nonché prevedere meccanismi per tracciare tutte le attività condotte sui dati; non solo, quindi, *log* di accesso come accade in Italia nel caso degli amministratori di sistema);
- **policy di controllo dei fornitori** (definire *policy* per controllare gli eventuali fornitori di servizi coinvolti nel trattamento dei dati biometrici, prevedendo ispezioni e controlli adeguati nei loro riguardi, richiedendo garanzie sul rispetto delle misure per gli incaricati di loro responsabilità e sulle procedure da attivare quando un interessato eserciti i diritti previsti dalla legge in merito al trattamento dei suoi dati).

Molte delle indicazioni proposte nell'Opinione del WP 29 trovano riscontro nei requisiti presenti nelle regole tecniche italiane in materia di firma elettronica avanzata.
Recentemente, tuttavia, anche l'Autorità Garante per la protezione dei dati personali italiana ha varato alcuni provvedimenti a conclusione di istanze di verifica preliminare (ex art. 17 d.lgs. 196/2003) avanzate da alcuni titolari del trattamento che operano nel settore bancario, autorizzando per la prima volta in Italia l'utilizzo dei dati biometrici legati alla firma (dati grafometrici) nell'ambito di sistemi di firma elettronica avanzata (FEA) o all'interno di procedimenti di sottoscrizione digitale da remoto.
È comunque utile che un eventuale futuro provvedimento di carattere generale del Garante per la protezione dei dati personali, relativo al trattamento dei dati biometrici - incluse le firme grafometriche -

stabilisca prescrizioni di misure e accorgimenti che possano favorire la conformità alle regole tecniche per la FEA da parte dei produttori di soluzioni e coloro che intendano erogare ai propri utenti servizi di FEA[26].
Tale provvedimento generale, riportante anche le linee guida per il trattamento di dati biometrici per scopi di autenticazione informatica, controllo degli accessi e sottoscrizione di documenti informatici, è al varo dell'Autorità Garante e fornirà tutte le prescrizioni e gli adempimenti necessari per gli operatori che vogliano erogare tale tipologia di servizi alla propria utenza.

[26] Giovanni Manca e Gloria Marcoccio, *"La firma grafometrica e l'Opinione dei Garanti Privacy Europei sui dati biometrici"* pubblicato su www.abirt.it (http://www.abirt.it/notizia/342_La_firma_grafometrica_e_l%E2%80%99Opinione_dei_Garanti_Privacy_Europei_sui_dati_bio.html).

3. Le firme elettroniche e la conservazione dei documenti informatici

3.1 Il valore giuridico e probatorio del documento informatico

Come accennato al paragrafo 1.1, nel nostro ordinamento sono disciplinati diversi tipi di firme elettroniche: queste contribuiscono a determinare il valore giuridico e probatorio dei documenti informatici a cui sono apposte.
I sistemi di firma elettronica, infatti, si differenziano non solo per le diverse tecnologie utilizzate, ma anche per la loro maggiore o minore capacità di assicurare la presenza di tutti gli elementi idonei a garantire che la manifestazione di volontà provenga da parte del soggetto firmatario, nonché l'integrità e l'immodificabilità del documento in tal modo firmato.

In effetti, a partire dal valore probatorio del documento informatico con firma elettronica semplice, l'articolo 21, comma 1, del CAD ha statuito che lo stesso è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza, integrità ed immodificabilità[27].

In particolare, con riferimento alla discrezionalità con cui il giudice sarà chiamato a valutare il documento firmato con una firma elettronica semplice, si dovranno considerare le peculiari caratteristiche tecniche, di volta in volta riscontrabili, in grado di avvicinare questa tipologia di firma elettronica in concreto utilizzata alla firma elettronica avanzata.

Al contrario della firma elettronica semplice, infatti, l'insieme di dati che connotano il processo di firma elettronica avanzata permette non solo l'identificazione del firmatario del documento, ma garantisce anche la loro connessione univoca al firmatario, in quanto creati con mezzi sui quali tale soggetto conserva un controllo esclusivo. Inoltre, il collegamento ai dati sottoscritti con la firma è tale da consentire di rilevare se i dati stessi siano stati successivamente modificati: in questo modo, a differenza della firma elettronica semplice, quella avanzata realizza un'unione inscindibile tra documento informatico e sua sottoscrizione[28].
Infatti, alle maggiori garanzie di qualità, sicurezza, integrità e immodificabilità offerte dai documenti informatici sottoscritti con sistemi di firme elettroniche avanzate viene dato adeguato risalto al comma 2 dell'art. 21 del CAD, che riconosce a questi tipi di documenti, così come anche a quelli sottoscritti con una firma qualificata o digitale, l'efficacia prevista dall'articolo 2702 del codice civile. L'efficacia probatoria riconosciuta ai documenti informatici sottoscritti con firma elettronica avanzata, qualificata o digitale è quindi quella della scrittura privata, pienamente valida in quanto "*l'utilizzo del dispositivo di firma si presume riconducibile al titolare* [della firma elettronica utilizzata]*, salvo che questi dia prova contraria*".

Tuttavia, lo stesso CAD, al comma 2 *bis* dell'art. 21, pone in rilievo le particolari caratteristiche di sicurezza dei sistemi di firma qualificata e digitale rispetto a quelli di firma elettronica avanzata, introducendo un limite all'utilizzo di queste ultimi per la valida sottoscrizione dei documenti informatici

---

[27] Sulla scorta della previsione comunitaria contemplata nella Direttiva 1999/93/CE, art. 5, comma 2, che imponeva agli Stati membri di non considerare inefficace e irrilevante il documento informatico con firma elettronica semplice.

[28] Cfr. B. Santacroce, *Dalla firma digitale alla firma biometrica: quadro giuridico di riferimento per l'applicazione dei nuovi dispositivi di firma*, cit.

contenenti le scritture private di cui ai numeri da 1 a 12 dell'art. 1350 del codice civile e prevedendo espressamente che per queste sia necessario l'utilizzo di una firma elettronica qualificata o digitale.

A questo punto, è opportuno richiamare la distinzione, comunque esistente, tra le differenti tipologie di firma elettronica avanzata: tra queste, infatti, si distinguono la firma qualificata, che è una firma avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, e la firma digitale, che invece è un particolare tipo di firma elettronica avanzata basato su un sistema di due chiavi crittografiche, una pubblica e l'altra privata.

In sintesi, secondo gli articoli 20, comma 1 *bis*, e 21, comma 1, del CAD, i documenti informatici non sottoscritti e quelli sottoscritti con firma elettronica semplice sono liberamente valutabili in giudizio, in quanto il loro valore probatorio e l'idoneità a soddisfare il requisito della forma scritta dipendono dalle loro caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità.

Diversamente, ai sensi del secondo comma dell'art. 21 del CAD, i documenti informatici sottoscritti con un sistema di firma elettronica avanzata, qualificata o digitale acquistano l'efficacia probatoria pari a quella della scrittura privata, di cui all'articolo 2702 del codice civile, costituendo piena prova della provenienza delle dichiarazioni da parte del titolare della firma con cui sono stati sottoscritti.

Inoltre, secondo quanto disposto dall'art. 21, comma 2 *bis* dello stesso CAD, con specifico riferimento ai documenti informatici destinati a porre in essere atti di costituzione e trasferimento dei diritti reali immobiliari (di cui ai numeri da 1 a 12 dell'articolo 1350 c.c.) è richiesta, a pena di nullità, la sottoscrizione con firma qualificata o digitale.

3.2 La conservazione digitale dei documenti

Affinché il documento informatico mantenga nel tempo il medesimo valore probatorio, è indispensabile un corretto processo di conservazione digitale.
In tal senso, il comma 2 dell'art. 3 della Bozza di Regole tecniche per il documento informatico[29], dispone infatti espressamente che "il documento informatico assume la caratteristica di immodificabilità se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione".
In particolare, al successivo comma 4 dello stesso articolo, si elencano le operazioni idonee a garantire le caratteristiche di immodificabilità e di integrità nel caso in cui i documenti informatici siano formati tramite l'apposito utilizzo di strumenti software[30]. Queste sono:

---

[29] Bozza di Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41 e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

[30] Nel caso di documento informatico acquisito per via telematica o su supporto informatico, o acquisito tramite copia per immagine su supporto informatico di un documento analogico, oppure ancora mediante copia informatica di un documento analogico, le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di memorizzazione in un sistema di gestione informatica dei documenti che garantisca l'inalterabilità del documento o in un sistema di conservazione. Nel caso di documento informatico formato tramite registrazione informatica delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente, oppure mediante generazione o raggruppamento, anche in via automatica, di un insieme di dati o registrazioni, (provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica), le caratteristiche di immodificabilità e di integrità sono determinate dall'operazione di registrazione dell'esito della

a) la sottoscrizione con firma digitale ovvero con firma elettronica qualificata;
b) l'apposizione di una validazione temporale;
c) il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa;
d) la memorizzazione su sistemi di gestione documentale che adottino politiche di sicurezza;
e) il riversamento in un sistema di conservazione.

Di particolare rilievo appare anche quanto previsto al comma 7 del sopracitato art. 3, il quale dispone che, qualora non sia già presente, al documento informatico immodificabile deve essere associato un riferimento temporale, elemento che peraltro rientra nell'elenco minimo dei metadati che devono essere associati al documento informatico immodificabile, in base al comma 9 dello stesso art. 3, insieme all'identificativo univoco e persistente, all'oggetto, al soggetto che ha formato il documento, nonché all'eventuale destinatario.

Per quanto concerne la correttezza dei processi di conservazione dei documenti informatici, il Codice dell'Amministrazione Digitale stabilisce che tutti i documenti, che per legge o regolamento devono essere conservati, possono essere riprodotti e conservati su supporto informatico e sono validi a tutti gli effetti di legge[31]. La loro riproduzione e relativa conservazione, infatti, devono essere effettuate in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo. Inoltre, qualora i documenti siano prodotti originariamente in modalità informatica, è obbligatorio che la loro conservazione permanente avvenga con modalità digitali (art. 43, comma 3, CAD).

Più in generale, la conservazione digitale può essere definita come quel procedimento che permette di assicurare la validità legale nel tempo a un documento informatico[32] o a un documento analogico digitalizzato. Nello specifico, conservare digitalmente il documento informatico significa garantire ad un documento digitale, già correttamente formato, l'autenticità, l'integrità e l'immodificabilità nel tempo, attraverso gli strumenti del riferimento temporale e della firma digitale del Responsabile della conservazione. Mentre l'utilizzo della firma digitale del Responsabile è necessario a validare il processo di conservazione, rendendo immodificabile il documento o l'insieme dei documenti affidati alla sua custodia, la validazione temporale, invece, permette di determinare temporalmente tale affidamento e di estendere la validità dei certificati di firma digitale.

Ovviamente, occorrerà sviluppare un processo che rispetti gli attuali parametri tecnici fissati dal DPCM 3 dicembre 2013. In base a tali norme, infatti, la conservazione digitale dei documenti informatici, a prescindere dalla loro natura di documenti nativamente informatici o di documenti analogici digitalizzati, deve avvenire mediante il loro versamento in un sistema di conservazione e la predisposizione e la successiva gestione di un pacchetto di archiviazione sottoscritto con firma digitale del responsabile della conservazione.

---

medesima operazione e dall'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema, ovvero con la produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

31 L'art. 43, comma 1, del CAD stabilisce che *"I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71"*.

32 Il documento informatico è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (lett. p), comma 1, art. 1 CAD).

Il Responsabile della conservazione digitale deve, inoltre, garantire la tracciabilità di tutte le operazioni effettuate durante l'intero processo; la tracciabilità consente, infatti, di facilitare le operazioni di controllo e verifica effettuate dagli organi preposti e di mappare più facilmente l'iter che il documento ha percorso, permettendo, altresì, di risalire ai vari soggetti che si sono interfacciati al sistema informatico dell'azienda.

Nello specifico, all'art. 44 del CAD sono elencati i requisiti minimi necessari per la conservazione dei documenti informatici, ossia:

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

b) l'integrità del documento;

c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;

d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

Inoltre, il comma 1 *bis* dell'art. 44 stabilisce che il sistema di conservazione deve essere gestito da un Responsabile della conservazione che lavori d'intesa con il Responsabile del trattamento dei dati personali, di cui all'art. 29 del D. Lgs. 196/2003 e, ove si tratti di documenti di una Pubblica Amministrazione, anche con il Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi[33].

Con particolare riguardo alle PA, l'art. 50 *bis*, inserito dall'art. 34, comma 2, del CAD, impone che le stesse adottino piani di continuità operativa e di *disaster recovery*, in modo da garantire, anche in situazioni di emergenza, "la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività". In ogni caso, il successivo art. 51, comma 2, del CAD dispone che i documenti informatici delle pubbliche amministrazioni siano custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

[33] Sul punto, il comma 1 *ter* dell'art. 44 dello stesso CAD, oltre a ribadire la possibilità che il processo di conservazione sia affidato in *outsourcing*, riconosce anche la possibilità che soggetti terzi certifichino la conformità di tale processo a quanto stabilito dall'art. 43 del CAD (Riproduzione e conservazione dei documenti) e dalle regole tecniche stabilite ai sensi dell'art.71 del codice medesimo. In merito a questo profilo, il successivo art. 44 bis prevede che i soggetti pubblici e privati, che svolgono attività di conservazione dei documenti e di certificazione dei relativi processi, possano accreditarsi presso DigitPa per conseguire il riconoscimento del possesso dei requisiti di livello più elevato in termini di qualità e sicurezza. Ovvia conseguenza di tale disposizione è quella di rendere processualmente più problematico il disconoscimento di una copia digitale sostitutiva di un originale analogico effettuata da un conservatore accreditato.

Principale normativa di riferimento

- Codice dell'amministrazione digitale di cui al Decreto Legislativo n. 82 del 2005
- Direttiva europea 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche
- Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013 (Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71)
- Deliberazione CNIPA 45/2009 così come modificata dalla Determinazione Commissariale DigitPA n. 69/2010 (*Regole per il riconoscimento e la verifica del documento informatico*)
- Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013 (Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005)
- D.lgs. 30 giugno 2003, n. 196 (*Codice in materia di protezione dei dati personali*)

Bozze di Regole tecniche

- Bozza di Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41 e 71, comma 1, del Codice dell'amministrazione digitale di cui al Decreto Legislativo n. 82 del 2005 e relativi allegati

Bibliografia essenziale

- A. Lisi, *Le nuove frontiere del documento informatico e della firma elettronica: dalla firma digitale attraverso quella grafometrica fino alla "mobile signature"*, in Sistemi&Impresa, n° 4, 2012;
- B. Santacroce, *Dalla firma digitale alla firma biometrica: quadro giuridico di riferimento per l'applicazione dei nuovi dispositivi di firma*, Minigrafia nr. 9 *Il nuovo CAD. Commenti e prospettive. Atti del Convegno dell'8 luglio 2011.* Roma, Accademia dei Lincei, edito dalla Fondazione Siav Academy;
- G. Manca, *Il decalogo della firma grafometrica,* in Information Security n° 8 gen-feb 2012;
- G. Manca e G. Marcoccio, *La firma grafometrica e l'Opinione dei Garanti Privacy Europei sui dati biometrici* pubblicato su www.abirt.it
- Andrea Lisi, Simonetta Zingarelli, Francesca Giannuzzi, Luigi Foglia, *Guida alla conservazione digitale dei documenti*, Edisef, 2011.

Sitografia essenziale

http://www.agid.gov.it/
www.anorc.it
www.abirt.it
http://www.esignaturelegalwiki.org/wiki/Main_Page
www.aifag.org

Profilo degli autori

Avv. Andrea Lisi: è coordinatore del Digital&Law Department dello Studio Legale Lisi (www.studiolegalelisi.it), Presidente ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti), Vice Presidente di ANORC Professioni e Segretario generale AIFAG (Associazione Italiana Firma elettronica Avanzata, Biometrica e Grafometrica**).** Già Docente di Informatica Giuridica nella Scuola di Professioni Legali, Facoltà di Giurisprudenza dell'Università del Salento, oggi è docente nella Document Management Academy, SDA Bocconi, Milano, al MIS Academy - Management Information System – SDA Bocconi – IBM, nel Master in Management della cultura digitale, editoria, archivi e biblioteche nell'era del 2.0, Università di Verona e di UniDOC- Progetto di formazione continua in materia di documentazione amministrativa, amministrazione digitale, delibere degli organi e documenti informatici - COINFO - Consorzio interuniversitario sulla formazione - Università degli Studi di Torino. Ha fondato il Centro Studi&Ricerche Scint www.scint.it e la prima banca dati sul diritto dell'informatica www.scintlex.it. È stato Direttore della "RIVISTA DI DIRITTO ECONOMIA E GESTIONE DELLE NUOVE TECNOLOGIE", Nyberg Editore, Milano e attualmente dirige la Collana "DIRITTO, ECONOMIA E SOCIETÀ DELL'INFORMAZIONE", Cierre Edizioni, Roma. Oggi è direttore editoriale della rivista IL DOCUMENTO DIGITALE pubblicata da Lex et Ars. Già componente del Comitato Scientifico nel Master in "DIRITTO DEL'INFORMAZIONE E DELL'INFORMATICA" presso l'Università di Messina (Direttore Prof. Trimarchi), oggi è nel Comitato Scientifico dell'Istituto Italiano per la Privacy (IIP) - http://www.istitutoitalianoprivacy.it, della Document Management Academy, SDA Bocconi, Milano, del DOCUBUSINESS (http://www.docubusiness.it), del Progetto e-HealthCare Forum (www.forumhealthcare.it), della Rivista Digital Document Magazine (edita da 4itGroup), del Centro Studi Themis Crime e di varie riviste giuridiche cartacee e telematiche ed è autore di diversi volumi e numerose pubblicazioni in materia di diritto delle nuove tecnologie. È stato, infine, docente in master dedicati al diritto dell'informatica presso la Business School del Sole24Ore, l'Università di Lecce, Taranto, Trento, Padova e Messina ed è iscritto all'Albo Docenti della Scuola Superiore dell'Amministrazione dell'Interno. Attualmente è arbitro di numerosi enti di risoluzione stragiudiziale delle dispute relative ai domini Internet ccTLD.it ed è Conciliatore Specializzato DM 23/07/2004 n. 222, è Esperto Valutatore IMQ per il servizio di attestazione Q&S_CS (Qualità e Sicurezza nella Conservazione Sostitutiva) e collabora in tutta Italia con università, enti camerali, centri di ricerca, primarie società fornendo progettazione, formazione, assistenza e consulenza legale nell'e-business internazionale, nella privacy, nei servizi di conservazione digitale/fatturazione elettronica, nella realizzazione dei modelli organizzativi D. Lgs. 231/2001 e nel diritto delle nuove tecnologie, in genere.

Avv. Luigi Foglia:
Avvocato dal 2009, collabora stabilmente con il Digital & Law Department dello Studio Legale Lisi, occupandosi principalmente di diritto dell'innovazione digitale, contratti ad oggetto informatico, formazione e conservazione digitale del documento informatico, firme elettroniche, fatturazione elettronica, innovazione nella PA, privacy, licenze d'uso software e disaster recovery. Collabora con le principali riviste italiane che affrontano i temi legati alla digitalizzazione. Delegato territoriale ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale dei Documenti).

Avv. Graziano Garrisi:
Avvocato dal 2008, fa parte del Digital & Law Department dello Studio Legale Lisi, occupandosi principalmente di consulenza legale in materia di privacy e diritto delle nuove tecnologie, nonché nella realizzazione dei modelli organizzativi D. Lgs. 231/2001 e D.Lgs. 196/2003. Socio fondatore e membro del Direttivo di ANORC (Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti) è Vice Coordinatore di ABIRT (Advisory Board Italiano dei Responsabili del Trattamento dei dati personali). Relatore in numerosi convegni e autore di pubblicazioni in materia di diritto delle nuove tecnologie.

Avv. Sarah Ungaro:
Avvocato del Foro di Lecce, ha conseguito il diploma della Scuola di Specializzazione per le professioni legali. Collabora con il D&L Department dello Studio Legale Lisi occupandosi prevalentemente di e-

government, formazione e conservazione digitale dei documenti informatici, cloud, fatturazione elettronica, privacy e della redazione di articoli e contratti.

Notaio Avv. Eugenio Stucchi:
Notaio con sede in Carmagnola (To) (uffici anche a Villastellone e Torino) è tra i soci fondatori della Associazione Italiana Giovani Notai.

Si occupa per passione e professione dei temi della digitalizzazione applicati alla professione notarile, e in tale ottica ha creato un software specifico per la pubblicazione e condivisione on line su area riservata degli atti notarili. È membro del Consiglio Direttivo della Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti (ANORC, www.anorc.it) e ha partecipato quale relatore a diversi convegni sulle tematiche della digitalizzazione documentale. Attualmente collabora con la Commissione Informatica del Consiglio Nazionale del Notariato a progetti di formazione e di studio.