Rivista elettronica di Diritto, Economia, Management
N. 1 - 2014 • pp. 50-62

Firme grafometriche e tutela dei dati personali

Gianluigi Ciacci

Multimedia

Clicca sull'immagine o fotografa il QrCode per accedere al MediaBook CLIOedu

Abstract: Nell'ambito del sistema italiano di validazione giuridica delle dichiarazioni elettroniche di recente si è affermata una nuova modalità di sottoscrizione in forma elettronica, quella delle c.d. firme grafometriche: modalità che è stata ritenuta inquadrabile tra le c.d. firme elettroniche avanzate secondo quanto stabilito dal Codice dell'Amministrazione Digitale e dalle nuove regole tecniche emanate con il D.P.C.M. 22 febbraio 2013. Le firme grafometriche sono quelle che utilizzano il rilevamento dinamico dei dati calligrafici (posizione, pressione, velocità, tempo, inclinazione della penna, accelerazione, movimento, …) della sottoscrizione di un individuo, acquisiti attraverso una penna elettronica, o comunque attraverso un tablet. Ma proprio il fatto di basarsi sull'acquisizione di informazioni di tipo comportamentale, e quindi di dati biometrici, rende questo nuovo sistema sottoposto alla disciplina del D.Lgs. 30 giugno 2003 n. 196, il Codice in materia di protezione dei dati personali: con una serie di criticità che vengono esaminate nel presente scritto, rielaborazione dell'intervento al Convegno dell'A.N.D.I.G. "I nuovi scenari della società dell'informazione: aspetti politici, giuridici, amministrativi e tecnici" tenuto a Roma il 29 ottobre 2013.

Recently a new type of electronic signature known as the "Graphometric Signature" has a growing relevance in Italy. It consists of a handwritten signature being added to a digital document by means of a tablet using a special pen. According to the Italian Digital Administration Code currently in force, and the new technical rules on electronic signatures issued with D.P.C.M. 22 febbraio 2013, this signature can be regarded as either an electronic signature or as an advanced electronic signature This technology saves the signature, digitally, but at the same time special sensors gather every detail of how a person actually signs its name: the speed, writing angle, pressure and even the rhythm of a person's signature is recorded, making it unique to each person and virtually impossible for the signature to be forged.

The technology used in graphometric signature systems involves the processing of biometric user data, and then it must be applied the italian Data Protection Code. This article examines criticality and problems of this application, analyzing recent decisions by the Italian Data Protection Authority concerning preliminary examination of these systems.

Parole chiave: documento elettronico, firme elettroniche, firme grafometriche, biometria, dati biometrici, protezione dei dati personali, Garante privacy, verifica preliminare

Il tema delle firme grafometriche si inserisce nel settore di studi relativo al valore giuridico del documento informatico, nato nel nostro Paese negli anni '80 e consolidatosi nella seconda metà degli anni '90 con l'introduzione del sistema di firma digitale (era il 1997) allo scopo di sottoscrizione elettronica. Firma digitale che si basava (in maniera trasparente per l'utente) sulla crittografia asimmetrica per acquisire certezza della provenienza, dell'imputazione di una determinata dichiarazione elettronica, e sulla c.d. funzione di hash per raggiungere il risultato della non ripudiabilità del testo, del contenuto di tale dichiarazione elettronica. L'applicazione di entrambe le tecniche permetteva quindi di equiparare, dal punto di vista del valore giuridico, il

documento elettronico firmato digitalmente al tradizionale documento cartaceo sottoscritto in maniera autografa.
Sedici anni dopo, a fronte della enorme diffusione delle tecnologie informatiche e telematiche, della sempre più affermata smaterializzazione dell'attività di documentazione, si è sentita la necessità di andare oltre, di superare la tecnologia della firma digitale (anche in conseguenza dell'evoluzione normativa di spinta comunitaria), e si sono create nuove e diverse modalità di sottoscrizione elettronica, come appunto quella delle firme grafometriche.
Queste sono una particolare tipologia di firma con strumenti informatici che utilizza il rilevamento dinamico dei dati calligrafici (posizione, pressione, velocità, tempo, inclinazione della penna, accelerazione, movimento,…) della sottoscrizione di un individuo, acquisiti attraverso una penna elettronica, o comunque attraverso un tablet. Tipologia che sta avendo di recente una repentina diffusione, tra l'altro perché consente di essere utilizzato senza nessuna preventiva predisposizione al sistema, e quindi senza costi, per il soggetto che firma.
Ma l'assenza di costi, e la maggiore facilità di utilizzo e gestione, non esime l'utente di tale metodologia dalla necessità di coordinare la propria iniziativa con specifiche discipline di settore ad essa in qualche modo collegate. Questo non solo per le fonti appositamente dedicate alla fattispecie (da ultimo il DPCM 22 febbraio 2013, le regole tecniche sulle firme elettroniche), ma con particolare riferimento alla normativa in materia di tutela dei dati personali, il D.Lgs. 30 giugno 2003 n. 196, poiché l'utilizzo delle firme grafometriche implica il trattamento di informazioni relative all'individuo: e quindi porta all'applicazione di quell'insieme di regole, spesso oscure e contraddittorie, che rientrano nella c.d. (seppure imprecisamente) "legge sulla privacy".
Nel presente scritto, premesso un breve approfondimento circa la tematica del valore giuridico del documento elettronico, delle firme elettroniche e delle firme grafometriche, affronteremo il problema dell'applicazione delle disposizioni del D.Lgs. 196/2003 al settore in esame, anche alla luce di alcune recenti pronunce dell'Autorità Garante per la protezione dei dati personali.

1. La gestione dell'attività di documentazione in forma elettronica e il suo valore giuridico.

Come si è detto, alla fine degli anni ottanta in Italia la sempre maggiore diffusione dell'informatica nei più diversi settori della collettività ha reso necessario stabilire quale valore giuridico dovesse essere riconosciuto all'attività di documentazione svolta in modo elettronico. Infatti, i principali istituti giuridici che venivano in modo più o meno spontaneo applicati ed osservati nella quotidianità erano stati concepiti per una realtà materiale, che tradizionalmente era quella cartacea, nella quale si riteneva necessaria la sottoscrizione autografa per ottenere l'imputazione di una determinata dichiarazione: elementi che rendevano possibile verificare la presenza dei requisiti di genuinità, sicurezza, provenienza e non ripudiabilità in un documento, necessari a dare ad esso una rilevanza giuridica. Dopo un intenso dibattito, ed un lungo periodo di studio e quindi di consolidamento della tematica, la soluzione che si è scelto di adottare nella seconda metà degli anni novanta per dare valore al documento elettronico è stata quella dell'adozione della c.d. firma digitale: sistema che ha visto dare rilevanza ad un procedimento puramente tecnico nell'ambito di una disciplina di

tipo giuridico per ottenere il risultato richiesto.
Per "firma digitale", in particolare, si deve intendere la sottoscrizione predisposta mediante elaboratore elettronico sulla base della tecnica della crittografia a chiave asimmetrica (anche detta a doppia chiave) e di una particolare funzione matematica (la c.d. funzione di hash): con la prima si raggiunge la certezza della provenienza della dichiarazione elettronica; con la seconda tecnica si ottiene invece la sicurezza che il testo della dichiarazione non sia stato alterato, che sia dunque integro, e di conseguenza non ripudiabile. Niente a che vedere quindi con la tradizionale sottoscrizione posta alla fine, o a margine, di un foglio di carta, né proprio con la firma autografa: in questo caso si tratta infatti di un sistema puramente tecnico che si basa sull'esclusività del suo uso, e non sull'univocità della calligrafia di firma, per rendere possibile l'imputazione di un documento elettronico. Sistema che costituisce oggi il criterio legale in base al quale è possibile far risalire ad un determinato soggetto un documento redatto attraverso il computer: criterio mediante il quale cioè l'ordinamento giuridico riesce ad attribuire il valore di piena prova alla documentazione prodotta, gestita e trasmessa utilizzando le nuove tecnologie dell'informazione e della comunicazione, prescindendo dalla necessità della relativa stampa, e quindi della relativa sottoscrizione autografa.
Risolto in questo modo il problema relativo all'efficacia dell'uso dell'informatica nell'attività di documentazione, negli anni successivi in diverse occasioni il Legislatore è intervenuto per modificare differenti aspetti del sistema italiano di validazione giuridica del documento elettronico: modifiche a livello tecnico (apertura a diverse tipologie di firme elettroniche oltre a quella digitale, quali la firma elettronica semplice, quella avanzata, quella qualificata) o giuridico (creazione di differenti valenze per le diverse realtà di documenti elettronici, a seconda della presenza o meno di una firma, e del tipo di questa), fino ad arrivare ai giorni nostri, in cui si può considerare abbastanza consolidata la situazione. Infatti, tralasciando la descrizione dell'indicata evoluzione normativa del sistema, oggi è possibile individuare sia gli strumenti per procedere nella sottoscrizione elettronica (ad esempio di una mail o di un modulo da compilare all'interno di un sito web), sia le diverse fattispecie legate al valore giuridico del documento elettronico, che si possono schematizzare in questo modo: con riferimento alle tipologie di firma, senza dilungarci nella precisa descrizione tecnica di ognuna di esse, si possono distinguere

- *la firma elettronica* (*semplice*), di cui può costituire esempio la digitazione del pin del bancomat insieme alla lettura della corrispondente tessera magnetica (per farsi riconoscere titolare del conto corrente bancario), o ancora il nome-utente e la password per accedere ad un determinato servizio (come nel caso di utilizzo della posta elettronica): si tratta di dati elettronici associati ad altri dati, ed utilizzati come metodo di identificazione informatica (la definizione completa è riscontrabile nell'art. 1, lett. *q*, del D.Lgs. 82/2005, il c.d. C.A.D., Codice dell'Amministrazione Digitale).
- *la firma elettronica avanzata* (F.E.A.), di cui oggi sembrerebbero rappresentare principale esempio le applicazioni di *firma grafometrica*, quelle cioè che vedono l'apposizione di una sottoscrizione autografa su tavoletta elettronica, in grande sviluppo soprattutto nel settore bancario: come si vedrà in maniera approfondita oltre, anche per la presente tipologia si tratta di dati in forma elettronica allegati, o comunque connessi, ad un documento informatico, creati con mezzi sui quali il firmatario ha un controllo esclusivo, che consentono la sua identificazione e allo stesso tempo di rilevare se gli stessi dati firmati siano stati successivamente modificati (anche in

questo caso si veda per la definizione precisa l'art. 1, lett. *q/bis*, del C.A.D.). Di recente alcune applicazioni di firma grafometrica, oltre ad identificare l'autore della sottoscrizione elettronica, consentono anche di ottenere l'imputazione della dichiarazione al suo autore, utilizzando tecniche proprie della successiva tipologia.

- *la firma elettronica qualificata*, di difficile individuazione autonoma dalla firma digitale, di cui al successivo punto, è una firma elettronica avanzata che utilizza dispositivi sicuri per la realizzazione della sottoscrizione elettronica, con l'intervento di società di certificazione di alto livello (per la definizione si veda l'art. 1, lett. *r* del C.A.D.): ne possono costituire esempi i sistemi di gestione a distanza dei rapporti bancari attraverso l'identificativo utente e il c.d. token, ed anche le applicazioni di firma grafometrica che uniscono agli strumenti di identificazione dell'autore anche quelli di imputazione certa della sua dichiarazione, ad esempio in campo sanitario per l'acquisizione del consenso informato medico.
- *la firma digitale*, che tra le varie tipologie è quella più affermata e consolidata (nel 2013 si sono raggiunti i 7 milioni di kit per firmare digitalmente distribuiti nel nostro Paese), è il ricordato sistema che utilizza la crittografia asimmetrica e la funzione di hash per raggiungere la certezza dell'autore della dichiarazione elettronica e la non ripudiabilità della stessa: al momento è possibile acquisirla da una decina di certificatori (tra cui Postecom, Aruba, Infocert, Actalis,…), con una spesa media annua di circa cinquanta euro, e si può utilizzare per diverse necessità, dalla partecipazione a concorsi pubblici, all'invio della dichiarazione dei redditi, alla notifica del trattamento dei dati personali al Garante della privacy.

Con riferimento ai diversi valori giuridici conseguibili usando, o meno, le indicate modalità di sottoscrizione elettronica (valori che in genere si rapportano all'idea di valutazione da parte di un giudice, e quindi ad una fase conflittuale del rapporto tra le parti, ma che chiaramente possono essere riferiti a situazioni operative e precedenti, o comunque che prescindono dal sorgere di una controversia), sulla base della disciplina dettata dagli artt. 20 e 21 del C.A.D. distinguiamo

- *documento elettronico predisposto senza una firma elettronica*: nel caso in cui tale documento si riferisca in qualche modo al suo autore (si pensi ad un form in cui viene compilato con i dati di chi lo invia), il suo valore è assimilabile a quello di prova legale se non viene disconosciuto dalla parte contro cui è prodotto, altrimenti sarà liberamente valutabile dal giudice che terrà conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabiltà del documento; *in pratica*, questo ha un suo valore di per sé, e in caso di contestazione nel rapporto può essere prodotto in giudizio come succede per quello cartaceo (anche se poi sarà probabilmente oggetto di controversia proprio la sua genuinità: cioè la parte che ha mandato il documento potrebbe negare di averlo fatto, o di averlo fatto con quel testo, spostando quindi l'onere di provarne l'autore al soggetto che l'ha ricevuto).
- *documento elettronico predisposto con una firma elettronica semplice*: anche in questo caso sarà la libera valutazione del giudice (che terrà conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità) a stabilirne il valore; rispetto al caso precedente si restringerebbe l'ambito di discrezionalità connesso al convincimento del giudice, perché il documento firmato, seppure con una firma-base, avrebbe un maggior grado di affidabilità. *In pratica*, l'aver previsto un sistema di sottoscrizione elettronica rende più semplice la gestione dell'eventuale azione giudiziaria di contestazione.
- *documento elettronico predisposto con una firma elettronica avanzata, qualificata o digitale*: in questo caso

si realizza la totale equiparazione tra documento cartaceo ed informatico, tra sottoscrizione autografa ed elettronica, ed in particolare il valore che si attribuisce, secondo quanto previsto dall'art. 21 comma 2 del C.A.D., è quello ex art. 2702 del codice civile, quindi di scrittura privata (che fa piena prova della provenienza della dichiarazione da chi l'ha sottoscritta). La differenza tra l'uno o l'altro tipo di firma, a parte le specifiche tecniche già indicate, influenza gli atti che devono essere firmati, e non il valore giuridico in sé: infatti per situazioni giuridiche particolarmente rilevanti (ad esempio, la compravendita di un immobile, o per gli atti previsti nell'art. 1350 nn. 1-12), è necessaria la firma più sicura, e quindi quella digitale, o comunque qualificata; per atti giuridici di rilevanza minore (ad esempio, un contratto di assicurazione o il patto di non concorrenza, atti previsti dall'art. 1350 n. 13) è sufficiente una firma elettronica avanzata. *In pratica*, se sorge una controversia, e viene prodotto in giudizio un documento elettronico a cui è stata apposta una firma digitale, o comunque una firma elettronica avanzata, il suo valore è assimilabile a quello di prova legale (se non viene disconosciuto dalla parte contro cui è prodotto: ipotesi in cui sarà però tale parte a dover dimostrare il motivo per cui il documento non gli si può imputare, e se non ci riesce si realizza la prova legale, cioè viene riconosciuto provato quanto affermato dalla parte che lo ha prodotto in giudizio): il giudice non sarà quindi più libero di valutare o meno affidabile quel documento, ma è obbligato a considerarlo come una scrittura privata.

Indicati i punti più rilevanti degli aspetti legali dell'attività di documentazione attraverso le nuove tecnologie dell'informazione e della comunicazione, si procederà ora ad esaminare una nuova applicazione di sottoscrizione elettronica, la firma grafometrica, che di recente ha avuto una rilevante diffusione nel nostro Paese. Diffusione che sicuramente dipende dalle sue caratteristiche (facilità ed economicità d'uso, ma soprattutto nessun onere per il soggetto che firma), ma che è anche legata al suo riconoscimento normativo, sia come sistema di sottoscrizione elettronica valido (rientrerebbe nella tipologia di firma elettronica avanzata introdotta dall'art. 1, comma 1, lett. q-bis del D.Lgs. 82/2005), sia in particolare come metodologia adatta alla sottoscrizione di una serie di atti giuridici individuati sulla base dell'art. 1350 n. 13 del codice civile.

2. La sottoscrizione elettronica mediante la firma grafometrica: caratteristiche, utilità, tipologie e valore giuridico.

Come si è detto, la firma grafometrica è quella particolare tipologia di firma con strumenti informatici che utilizza il rilevamento dinamico dei dati calligrafici della sottoscrizione di un individuo (e quindi la posizione della penna, la sua inclinazione, la pressione del segno grafico, la velocità del movimento, la sua accelerazione, il tempo complessivo,…), acquisiti attraverso una penna elettronica, o comunque attraverso un tablet.

In tale sistema il soggetto che firma non dovrà preventivamente dotarsi di alcun dispositivo tecnico, evitando da una parte di doverne sostenere i costi, dall'altra di affrontare le complicazioni gestionali normalmente connesse all'utilizzo degli strumenti necessari ai medesimi scopi (ad

esempio per munirsi di un dispositivo di firma elettronica qualificata, o di firma digitale; poi per conservarlo in maniera sicura nel tempo; infine, per ricordarsi di "portarselo dietro" nel momento in cui si decida di utilizzarlo, rendendo quindi praticamente impossibile utilizzi estemporanei dello stesso): molto semplicemente, in alcune situazioni (ad esempio in banca, oppure alla reception di un albergo o alla cassa di un negozio, o ancora in altre specifiche realtà, come nel caso di consegne postali, o per la sottoscrizione del consenso informato medico), ci si troverà davanti ad una tavoletta grafica con penna elettronica, oppure ad un tablet con pennino, e si procederà a sottoscrivere un determinato testo apparso a video, di cui si è presa visione, praticamente come se si utilizzassero i tradizionali strumenti della carta e della penna.

Chi dovrà attivarsi per dotarsi dei dispositivi di firma, e per organizzare sotto diversi punti di vista un sistema di firma grafometrica, sarà chi vuole usufruire dei vantaggi di tale tecnologia (che sono diversi e di rilevante importanza, come si vedrà oltre): così, ad esempio, la banca, l'albergo, il negoziante o il medico che deve raccogliere il consenso informato del proprio paziente per iscritto. Soggetti che dovranno svolgere un'attività di predisposizione della propria struttura che implica certamente la necessità di occuparsi da una parte di diversi aspetti tecnici (dalla scelta del fornitore del sistema, alla decisione relativa alla finalità che si vuole raggiungere, …), e dall'altra di alcune procedure giuridiche, in particolare conseguenza del fatto che i dati grafometrici sono di natura biometrica, come si approfondirà nel successivo capitolo.

Con riferimento alle utilità collegate all'uso di questa tipologia di firma, a parte quanto già riportato nella descrizione delle caratteristiche del sistema, e quindi la maggiore semplicità per colui che firma (specifica che le rende adatte a certe necessità, e non ad altre: ad esempio, è inutile nel caso i soggetti debbano sottoscrivere documenti informatici occasionalmente e a distanza, mentre è molto utile per le sottoscrizioni da porre in essere "in presenza"), si può rilevare la migliore efficacia rispetto ai tradizionali e corrispondenti sistemi "analogici", cartacei. Infatti, secondo quanto riportato dalle società che forniscono sistemi di sottoscrizione grafometrica, nel caso di accertamento periziale su un documento cartaceo firmato in maniera autografa da un soggetto, le percentuali "di vero", cioè la possibilità di acquisire la certezza circa l'autenticità della sottoscrizione è pari al 60-65 %; mentre, nel caso si debba procedere ad un simile accertamento di una firma grafometrica su un documento informatico la percentuale di vero è superiore, nella specie intorno al 90-95 % (risultato conseguito perché all'analisi tradizionale a livello grafico del perito si sommano gli altri parametri resi possibili da specifici software che agiscono nel sistema). Quindi risulta essere più "sicura" una firma realizzata con l'ausilio di tale tecnologia rispetto a quella tradizionale analogica.

Deve essere infine considerato anche il minore costo complessivo del sistema: se infatti il soggetto che riceve le sottoscrizioni, e che dunque adotta il processo di firma grafometrica, sosterrà una spesa superiore, sarà però l'unico ad essere gravato di un costo (e comunque tale costo verrà bilanciato dal maggiore vantaggio, anche economico, conseguito a causa dell'esponenziale aumento del numero di soggetti che firmeranno i suoi documenti informatici), non dovendo spendere nulla il soggetto che invece firma.

Al momento le firme grafometriche vengono utilizzate, in tale ambito, con due diverse finalità, rispetto alle quali variano anche le modalità di uso dei relativi dati grafometrici:

- *a fini di identificazione*, di autenticazione: è la metodologia attualmente più diffusa, la sottoscrizione grafometrica viene utilizzata per riconoscere il soggetto che firma, in modo da consentirgli

di realizzare un determinato scopo (come ad esempio l'effettuazione di un bonifico dal proprio conto presso un istituto bancario). In essa le informazioni grafometriche (cioè quelle corrispondenti al rilevamento dinamico dei dati calligrafici della firma dell'individuo) acquisite grazie al dispositivo di firma sono accessibili dal soggetto che riceve la firma, e da questo conservate, poiché devono essere ogni volta confrontate con l'originario *spécimen*: il soggetto che fa firmare, e quindi riceve e conserva quei dati (ad esempio una banca), può dunque accedere, e di fatto accede, sia al dato grafometrico originario, sia a quello creato nella specifica occasione (entrambi parametri per effettuare il confronto e procedere nell'identificazione);

- *a fini di imputazione*, dichiarativi: è la metodologia che negli ultimi mesi sta avendo un forte sviluppo, in cui la sottoscrizione grafometrica è utilizzata per ricondurre una dichiarazione elettronica ad un determinato soggetto, suo autore (ad esempio, per acquisire l'accettazione di un'offerta contrattuale, oppure per raccogliere il consenso informato ad una prestazione sanitaria). Il funzionamento è diverso dalla precedente ipotesi: infatti i dati grafometrici non sono disponibili al soggetto che riceve la firma, il cui interesse all'accesso è solo eventuale, e unicamente nel caso il firmatario contesti di aver sottoscritto la determinata dichiarazione elettronica (ad esempio, il modulo del consenso informato alla prestazione sanitaria, oppure la dichiarazione di accettazione negoziale). In tale applicazione interviene una terza parte, che svolge il compito di rendere inaccessibile il dato grafometrico al soggetto che lo detiene, usando la tecnica della crittografia asimmetrica, ed eventualmente renderlo di nuovo accessibile nel momento in cui si attivi una procedura giudiziaria (ipotesi quindi legata ad un preciso ordine dell'autorità giudiziaria che richieda appunto l'acquisizione del dato): così in tale utilizzo si verifica la situazione che vede il soggetto che detiene il dato grafometrico non in grado di accedervi perché criptato, mentre il soggetto che ha la possibilità di decriptarlo non ha però la disponibilità del dato.

Con riferimento al valore giuridico delle firme grafometriche, innanzitutto esse possono essere pacificamente considerate quali firme elettroniche (semplici), e dunque come indicato in precedenza il loro valore è quello di prova legale se non vengono disconosciute dalla parte contro cui sono prodotte; in caso contrario, il livello probatorio sarà liberamente valutabile dal giudice che terrà conto delle caratteristiche oggettive di qualità, sicurezza, integrità e immodificabiltà del documento firmato con lo strumento grafometrico. Ma le firme grafometriche possono essere considerate anche quali firme elettroniche avanzate ai sensi dell'art. 1, lett. *q/bis*, del C.A.D., e con il valore probatorio stabilito dal suo art. 21 (scrittura privata ex art. 2702 del codice civile) ?

Per rispondere a questa domanda occorre fare riferimento a quanto disposto dal D.P.C.M. 22 febbraio 2013, le "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali (…)", il cui art. 56 elenca le caratteristiche che deve avere una soluzione F.E.A. per essere considerata tale. In particolare, i requisiti ritenuti necessari sono:

l'identificazione del firmatario del documento, la connessione univoca della firma al firmatario, il controllo esclusivo del firmatario del sistema di generazione della firma (ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima), la possibilità di verificare che l'oggetto della sottoscrizione non abbia subito modifiche dopo l'apposizione della firma, la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto, l'individuazione del soggetto di cui all'art. 55 comma 2 lettera *a* (n.d.r., cioè chi commercializza la soluzione di firma

grafometrica), l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati, la connessione univoca della firma al documento sottoscritto.
A fronte dunque dell'applicazione del principio di neutralità tecnologica stabilito per la firma elettronica da parte del C.A.D., in base al quale non viene richiesto l'utilizzo di una determinata tecnologia per realizzarla, se la specifica soluzione adottata corrisponde a quanto previsto dall'art. 56 delle citate regole tecniche, la risposta al quesito sarà affermativa: e quindi sarà possibile considerare come firma elettronica avanzata la firma grafometrica, e sottoscrivere con tale modalità gli atti individuati sulla base dell'art. 1350, n. 13, del codice civile (ad esempio un contratto di assicurazione, il compromesso che demanda una controversia alla soluzione arbitrale, il consenso informato al trattamento sanitario,…).
Individuato il fondamento giuridico all'uso di tale soluzione tecnica, a fronte della sua indubbia utilità pratica ed efficacia tecnologica, occorre a questo punto analizzare un ulteriore aspetto del processo di sottoscrizione grafometrica che solleva diverse difficoltà: questa volta non tanto rispetto alla disciplina del valore giuridico del documento elettronico, quanto per il differente settore della protezione dei dati personali del firmatario. Infatti, il ricordato rilevamento dinamico dei dati calligrafici (posizione, pressione, velocità, tempo, inclinazione della penna, accelerazione, movimento, …) della sottoscrizione di un individuo, portando all'acquisizione di informazioni di tipo comportamentale su quell'individuo, e quindi di tipo biometrico, realizza appunto un trattamento di dati biometrici, disciplinato in maniera specifica dal D.Lgs. 30 giugno 2003 n. 196, il Codice in materia di protezione dei dati personali.

3. Le firme grafometriche come firme biometriche: la biometria e protezione dei dati personali.

Per comprendere appieno il motivo per cui anche in questa fattispecie di sottoscrizione elettronica si debba applicare la disciplina in materia di dati personali, occorre muoversi dal concetto di "biometria", o meglio di dato biometrico. Devono infatti considerarsi tali le proprietà biologiche, gli aspetti comportamentali, le caratteristiche fisiologiche, i tratti biologici o le azioni ripetibili laddove tali caratteristiche e/o azioni sono tanto proprie di un certo individuo quanto misurabili, anche se i metodi usati nella pratica per misurarli tecnicamente comportano un certo grado di probabilità (definizione riportata nel parere del Gruppo art. 29 n. 3/2012 sugli sviluppi nelle tecnologie biometriche adottato il 27 aprile 2012): ne costituiscono esempi le impronte digitali, l'impronta retinica, l'analisi del DNA, il riconoscimento del volto o dello schema delle vene, e, tra gli aspetti comportamentali, proprio le firme grafometriche. Più nel dettaglio, il dato biometrico presenta tre caratteristiche del tutto peculiari: l'*universalità*, posto che l'elemento biometrico è presente in ciascun individuo; l'*unicità*, atteso che la componente biometrica è distintiva di ogni persona; la *permanenza*, dato che ognuno tendenzialmente conserva la propria caratteristica biometrica nel tempo.
Le tecnologie biometriche sono strettamente connesse a talune qualità personali degli individui, essendo i dati biometrici direttamente collegati al soggetto, alcune delle quali possono essere

utilizzate anche per rilevare dati sensibili (ne costituisce esempio il riconoscimento del volto, che permette di acquisire l'origine razziale del soggetto ritratto): molte di esse permettono poi anche il tracciamento automatizzato, nonché la profilazione delle persone, per cui il loro impatto potenziale sulla vita privata e sulla protezione dei dati delle persone è elevato. Si distinguono, in tale ambito, tecniche di tipo fisico e fisiologico (come per la verifica delle impronte digitali, l'analisi della retina, il riconoscimento del volto, della geometria della mano o della forma dell'orecchio, il rilevamento dell'odore del corpo, il riconoscimento vocale, l'analisi della struttura del DNA, …), di tipo comportamentale (ad esempio la verifica della firma manoscritta, l'analisi dell'andatura, il modo di camminare o di muoversi, schemi che indicano percorsi mentali subconsci come il fatto di mentire,…), ed infine quelle basate sulla psicologia, settore emergente in cui rientra la misurazione della risposta a situazioni concrete o test specifici per l'eventuale corrispondenza a un determinato profilo psicologico.

È importante ancora distinguere tra identificazione e autenticazione biometrica. Nel primo caso si è in presenza di un processo in forza del quale un sistema riconosce un individuo, e ne accerta l'identità, confrontando i dati del medesimo con una serie di modelli biometrici: dando, quindi, risposta alla domanda: "Chi è Tizio ?". L'autenticazione biometrica è invece il processo finalizzato a verificare che l'incaricato che chiede di accedere ad un determinato sistema sia effettivamente colui che dichiara di essere, attraverso il confronto dei suoi dati biometrici con quelli di un unico modello: dando, quindi, risposta alla domanda: "Tizio è la persona che dichiara di essere ?".

Il trattamento dei predetti dati richiede elevate cautele per prevenire possibili pregiudizi a danno degli interessati. Ma questo non significa che, in via generale, la normativa in materia ne impedisca l'utilizzo: stabilisce invece gli ambiti di trattamento consentiti in determinate condizioni, e le modalità concrete di questo, facendo rientrare tale tipo di trattamento di dati nei parametri tipici della stessa disciplina, applicando in particolare i principi generali della stessa.

Così, la finalità del trattamento è considerato un requisito fondamentale per il ricorso alla biometria: consiste nella chiara definizione degli scopi per i quali vengono raccolti e trattati i dati, tenendo conto dei rischi per la protezione dei diritti fondamentali e delle libertà delle persone. Anche con riferimento al principio di proporzionalità, deve essere valutata ogni categoria di dati trattati alla luce delle finalità del trattamento, considerando una serie di fattori: se il sistema è essenziale per soddisfare tale necessità o, piuttosto, se è solo il più conveniente; se il conseguente aumento della possibilità di lesione del dato personale sia proporzionata al vantaggio previsto; se esista un mezzo potenzialmente meno lesivo, o comunque meno invasivo della riservatezza, che possa raggiungere lo scopo desiderato. Il rispetto poi del principio di accuratezza implica l'attenzione al fatto che i dati biometrici trattati debbano essere accurati e pertinenti rispetto alle finalità per le quali vengono rilevati. E l'applicazione di quello di "minimizzazione dei dati", alla luce del fatto che spesso i dati biometrici contengono più informazioni di quelle richieste per il confronto delle funzioni, porta il titolare del trattamento biometrico a prestare attenzione, da una parte, a che soltanto le informazioni richieste debbano essere trattate, trasmesse o conservate, e non tutte quelle disponibili; e, dall'altra, che la configurazione di partenza del sistema biometrico agevoli la protezione dei dati.

Anche con riferimento alla durata del trattamento si applicano le regole generali: così, il titolare deve determinare un periodo di conservazione per i dati biometrici che non dev'essere superiore a quello necessario al conseguimento delle finalità per le quali essi sono rilevati o sono successivamente trattati; al termine del quale deve essere garantito che le informazioni o i profili derivati da tali

dati siano cancellati definitivamente (differenziando tra i dati generici che può conservare, e quelli biometrici non più utili che deve cancellare).
A parte l'applicazione dei principi generali della disciplina in materia di protezione delle informazioni personali, il trattamento dei dati biometrici implica la necessità di adeguarsi ad alcune sue previsioni specifiche, adempiendo ai rispettivi obblighi.
Infatti per il Codice in materia di protezione dei dati personali l'utilizzo delle informazioni biometriche deve essere inteso come un'attività "che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato", a cui quindi si applica il disposto del suo art. 17: e dunque chi vuole procedere in questo tipo di attività deve sottoporre a verifica preliminare dell'Autorità Garante per la protezione dei dati personali la sua intenzione. Verifica che verterà sulla presenza di quei requisiti che si sono indicati in precedenza.
Superata la verifica preliminare dell'Autorità (tenendo presente che, secondo il Provvedimento dell'8 aprile 2010 in tema di videosorveglianza, il Titolare è espressamente esonerato dal c.d. *prior checking* qualora il Garante si sia già espresso con un provvedimento di verifica preliminare in relazione a determinate categorie di titolari o di trattamenti) occorrerà procedere alla notifica dell'attività di trattamento alla medesima Autorità sulla base dell'art. 37, e quindi porre in essere gli altri adempimenti previsti dal D.Lgs. 196/2003. In particolare, predisporre e somministrare l'esplicita informativa al soggetto i cui dati si vogliono trattare, ed acquisirne il consenso, organizzando comunque modalità alternative in caso di rifiuto di tale consenso. Tutto questo tenendo presente che le sanzioni, in caso di inosservanza di tali specifiche previsioni, sono di notevole entità. Nella specie, la mancata richiesta di verifica preliminare è sanzionata, se dal fatto deriva nocumento, con la reclusione da uno a tre anni, e comunque con il pagamento di una somma da 10.000 a 120.000 euro e (così gli artt. 167, comma 2, e 162, comma 2-*bis*, del D.Lgs. 196/2003); ed anche la mancata notificazione ha una conseguenza sanzionatoria rilevante, e cioè il pagamento di una somma da 20.000 a 120.000 euro (art. 163).
Il Garante per la protezione dei dati personali si è di frequente pronunciato sulle attività di trattamento di dati biometrici, sia in fase di verifica preliminare ex art. 17 del D.Lgs. 196/2003, sia in fase di svolgimento della sua attività ispettiva; ed ha anche pubblicato alcune linee guida relative ad ambiti concettuali affini (si pensi alle Linee guida per il trattamento di dati dei dipendenti privati, Provvedimento 23 novembre 2006, e alle Linee Guida sul rapporto di lavoro pubblico, Provvedimento 10 luglio 2007). Da tale produzione si evince che l'Autorità distingue l'uso dei dati biometrici a fini di autenticazione, e quindi essenzialmente come misura di sicurezza prevista espressamente dalla Regola 2 dell'Allegato B del D.Lgs. 196/2003, da quello a fini di individuazione, cioè come sistema utilizzato per diverse utilità: nel primo caso, accertato il rispetto delle Regole 1-11 dell'Allegato B, l'attività di trattamento dei dati biometrici è stata considerata legittima di per sé; nel secondo caso il trattamento è stato ammesso solo in casi particolari, tenuto conto delle finalità e del contesto in cui sono stati utilizzati dati biometrici (e la verifica preliminare ex art. 17 del D.Lgs. 196/2003 è stata ritenuta essenziale).
In sintesi, la posizione del Garante nei confronti delle nuove applicazioni tecnologiche che sempre più portano all'impiego di informazioni dell'individuo di tipo biometrico è di attento controllo, cercando di allineare le varie esperienze ai principi "tipici" stabiliti dalla legge, anche se in alcune situazioni questo può portare (o porta) ad alcune difficoltà, come nel caso delle firme grafometriche.

4. Le pronunce del Garante per la protezione dei dati personali sui sistemi di firme grafometriche.

Infatti, come si è visto, il testo vigente del Codice dell'Amministrazione Digitale e le nuove regole tecniche in materia di firme elettroniche, emanate con D.P.C.M. 22 febbraio 2013, hanno conferito fondamento giuridico al sistema delle firme grafometriche, sistema che dunque può farsi rientrare tra le firme elettroniche avanzate. Ma è stato già evidenziato il fatto che tale metodo di sottoscrizione elettronica si basa sull'utilizzo di dati grafometrici che hanno natura biometrica, e che quindi implicano l'applicazione della disciplina sulla protezione dei dati personali: nella specie, tra le diverse norme che prevedono l'adempimento di specifici obblighi in capo al titolare, deve essere tenuta in particolare considerazione quella dell'art. 17 del D.Lgs. 196/2003, in cui si stabilisce l'obbligo di verifica preliminare da parte del Garante per i trattamenti che presentano "rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare".
Si tenga presente che l'analisi dell'Autorità nell'ambito del c.d. "*prior checking*" non si limita unicamente alla modalità di trattamento dei dati personali nel sistema oggetto di verifica, ma si estende all'opportunità stessa dell'adozione dello specifico sistema biometrico: situazione che si viene a creare quando viene valutata, rispetto al sistema sottoposto all'esame, la corretta applicazione dei principi di necessità, proporzionalità, pertinenza e non eccedenza. Con riferimento al caso di specie tale valutazione potrebbe sollevare un problema di coordinamento tra diverse discipline normative: si potrebbe cioè creare l'anomala situazione in cui il Garante ritenga non corretto un particolare trattamento di dati biometrici di un sistema di firme grafometriche perché ritenuto non necessario per principio, o comunque eccedente la finalità dichiarata, addirittura a prescindere dalla valutazione stessa delle modalità con cui vengono utilizzate le informazioni personali coinvolte. Modalità che potrebbero essere ritenute adeguate dal punto di vista degli obblighi relativi alle misure di sicurezza, o di quelli nei confronti dell'interessato (informativa e raccolta del consenso), ma poi ricevere una verifica preliminare con esito negativo perché viene ritenuto che lo stesso risultato si potrebbe ottenere con metodologie di firma tradizionali. E questo a prescindere dall'esistenza di altre regolamentazioni giuridiche di settore, come quelle del Codice dell'Amministrazione Digitale.
Per comprendere quanto alto sia il rischio del realizzarsi di tale anomalia si deve analizzare la produzione del Garante in sede di verifica preliminare ex art. 17 di sistemi di firma grafometrica: ricordando le due diverse finalità di utilizzo di tali sistemi di sottoscrizione, da una parte quella di autenticazione/identificazione, dall'altra quella di imputazione/dichiarativa. Nel primo caso il Garante, con provvedimento 31 gennaio 2013 su richiesta di Unicredit, ha ammesso il trattamento dei dati biometrici connesso all'uso della metodologia di firma grafometrica, ma legandolo alla specifica fattispecie esaminata ("… a condizione che esso avvenga per le sole finalità dichiarate, con le modalità indicate in narrativa e nel doveroso rispetto di quanto dichiarato dall'istante ai sensi dell'art. 168 del Codice"); e ad una soluzione simile è giunto anche nel recente provvedimento del 23 gennaio 2014 su richiesta di Telecom Italia Trust Technologies s.r.l. e Banca Generali S.p.A., in cui è entrato maggiormente nelle specifiche della fattispecie sottoposta a verifica, con riferimento alla titolarità del trattamento posto in essere nel sistema di firma grafometrica, all'informativa

e al consenso da predisporre per gli interessati (evidenziando la necessità di lasciare in ogni caso la possibilità di usare anche modalità di sottoscrizione "tradizionale" su moduli cartacei), alla conservazione dei dati biometrici di questi ultimi. Per entrambe le situazioni l'Autorità ha poi richiesto l'adozione di "particolari cautele a difesa dei dati biometrici degli utenti, anche in considerazione del fatto che parte del trattamento avverrà attraverso strumenti, tablet, che possono essere utilizzati in mobilità" (nella specie cautele che si concretizzerebbero nella protezione degli apparati utilizzati in modo di impedire che possano essere installati software non autorizzati o che vengano infettati da virus informatici, e predisponendo la possibilità del c.d. "*remote wiping*", cioè la possibilità di cancellare da remoto il contenuto del tablet nel caso in cui venga manomesso, smarrito o rubato).

Nella seconda ipotesi di utilizzo, in cui lo strumento grafometrico è usato per l'imputazione della dichiarazione elettronica, si registra al momento una sola decisione, quella del 12 settembre 2013 su richiesta di Fineco, che ha autorizzato il sistema ritenendo che questo trattamento dei dati biometrici non risulti connotato da specifici ed evidenti rischi per gli interessati, sempre se effettuato con le misure di sicurezza previste dalla legge; che l'utilizzo della soluzione proposta può contribuire a conferire maggiore certezza nei rapporti giuridici intercorrenti con gli utenti (in particolare dove è richiesta la forma scritta *ad substantiam*); che la firma grafometrica "asseconda legittime esigenze organizzative della società"; che comunque dovranno essere rispettati i diversi obblighi stabiliti dalla legge (ad es. per notificazione, informativa, consenso, misure di sicurezza,…).

Dall'analisi delle pronunce fin qui pubblicate dall'Autorità non si evidenzia quindi il contrasto di cui si è parlato: non ultimo perché in tutti e tre i casi la verifica è stata positiva. E a breve il Garante pubblicherà un provvedimento generale sul trattamento dei dati biometrici che probabilmente affronterà anche le problematiche delle firme grafometriche. Ma certamente anche la semplice possibilità che si crei il conflitto tra le due discipline richiamate deve portare gli operatori del settore, e i futuri utenti della tecnologia delle firme grafometriche, a prestare una maggiore ponderatezza circa gli aspetti di protezione dei dati personali dei soggetti firmatari coinvolti nei vari sistemi grafometrici.

D'altro canto si auspica che anche il Garante per la protezione dei dati personali, in sede di verifica preliminare ex art. 17 del D.Lgs. 196/2003, oppure nell'ambito del provvedimento generale di prossima pubblicazione, presterà attenzione soprattutto alle modalità di trattamento dei dati personali nelle differenti tipologie di firma grafometrica, e non tanto all'opportunità del sistema in sé. Tranne comunque sottoporre ad un'ulteriore riflessione ed approfondimento proprio la modalità di valutazione dei principi di necessità, proporzionalità, pertinenza e non eccedenza rispetto a questo specifico ambito di trattamento dei dati biometrici, che si ritiene debba avvenire in maniera evolutiva e non necessariamente in contrasto con il sempre maggiore sviluppo dell'innovazione tecnologica.