Firma Grafometrica

Una nuova stagione per i falsari

Premessa

La biometria è una disciplina interessante.

C'è qualcosa di intrigante nel fatto che sia possibile misurare alcune caratteristiche biologiche o comportamentali di un individuo ed utilizzare queste informazioni per un riconoscimento automatico dello stesso.

Come tutti sappiamo, nell'uso di questa disciplina ci sono alcuni margini di errore da prendere in considerazione, ma la tecnologia attuale, i protocolli in uso e l'integrazione di eventuali altri elementi di identificazione/ autenticazione, rendono la biometria uno strumento realmente utilizzabile.

La grafologia in ambito forense, cioè la tecnica di confrontare le forme e la dinamica dei segni grafici allo scopo di valutare la autenticità di una scrittura, rientra nel campo della biometria.

Questa tecnica valuta la naturalezza, la continuità, gli stacchi, le proporzioni, le dimensioni ed infine la pressione e la velocità di un segno grafico.

Fino a ieri, l'unica possibilità per verificare se un individuo fosse o meno l'autore di un documento autografo, era quella di fargli scrivere dell'altro testo di suo pugno, per poi fornire entrambi i documenti ad un perito grafologo.

Con l'aiuto della propria esperienza e magari di un microscopio stereoscopico, il perito grafologo, osservava attinenze, impostazioni, forme, pressione, continuità del tratto etc... per poi esprimere il suo parere sulla corrispondenza o meno dell'autore.

Oggi l'incontro con l'informatica, tipicamente l'uso di tavolette grafiche, ha reso il compito di un perito grafologo più confortevole, fornendo misurazioni oggettive (valori numerici) delle caratteristiche del segno grafico.

Inoltre rispetto all'analisi di un documento autografo, l'uso di una tavoletta grafica fornisce ad un perito grafologo, la misura certa di un elemento che prima dell'uso di questa tecnologia poteva solo intuire: il tempo utilizzato sia nelle operazioni di scrittura che nelle pause.

Tutto ciò rende più certa la valutazione del perito.

Peccato che di una tecnologia così affidabile e comoda nel supporto ad una perizia forense, si sia pensato di farne uno strumento per costruire sistemi di firma elettronica avanzata, tipicamente definiti con il termine di “Firma Grafometrica”.

Mi rendo conto che l’eliminazione dei documenti cartacei, abbia conseguenze economicamente interessanti per le grandi aziende e le istituzioni.

Mi rendo conto che la diffusione della firma qualificata[1], continua ad essere limitata da una serie di ostacoli che l’utente finale incontra, quando si vuole dotare di questo strumento ed anche quando lo vuole utilizzare nella pratica.

Mi rendo conto che la gestualità di una firma autografa, se pur apposta su una tavoletta grafica, risulta facile e familiare a chiunque e non genera nessun tipo di barriera culturale.

mi rendo conto di tutto.

Personalmente però, reputo questo approccio --almeno alle condizioni attuali-- assolutamente azzardato.

Penso che l’accettazione di un processo relativo ad una firma elettronica avanzata -basata sull’uso della tecnologia grafometrica- esporrà il singolo cittadino al consistente rischio di vedere utilizzata a sua insaputa la propria firma, in una modalità tale che gliene sarà praticamente impossibile il disconoscimento.

Di seguito proverò a chiarire il perchè di questa convinzione.

Firma elettronica avanzata [FEA]

Consideriamo la definizione prelevata dal Codice dell’amministrazione digitale all’Art.1 c.1 punto q-bis), recita:

firma elettronica avanzata: 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;

e poi l’Art.21 c.2 del codice:

Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all' articolo 20, comma 3 , che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile . L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria.

---

[1] per firma qualificata qui si intende una firma elettronica qualificata ovvero una firma digitale -ambedue basate su certificato qualificato- secondo le definizioni del DLgs 7 marzo 2005 n.82 (CAD); implicitamente ambedue prevedonp l’utilizzo di una device sicura per la creazione della firma (SSCD)

Diciamo che a fronte delle caratteristiche richieste all'art.1, una FEA potrebbe essere costruita con un sistema tecnicamente equivalente a quello utilizzabile per realizzare una firma qualificata, il quale però faccia uso di un certificato di chiave pubblica associato ad una persona giuridica.

Il certificato di questo tipo, andrebbe sempre emesso da un certificatore con i corretti requisiti di affidabilità e solvibilità, ma non sarebbe un certificato qualificato e quindi la firma elettronica risultante non sarebbe più identificabile come firma qualificata (firma elettronica qualificata o firma digitale).

Rimarrebbe quindi identificabile come un sistema di FEA con tutte le caratteristiche richieste dal codice.

Al contrario, analizzando quanto viene pubblicato e presentato dai fornitori di soluzioni di firma grafometrica --e sto pensando naturalmente solo a fornitori seri e preparati-- molti conti sembrano non tornare.

Prima di tutto l'ipotesi che il firmatario possa conservare un controllo esclusivo dei mezzi con i quali si creano i dati della firma elettronica avanzata, a fronte delle implementazioni proposte dai fornitori, sembra una ipotesi assolutamente irraggiungibile.

In secondo luogo, almeno a me sembra più che plausibile creare false firme, impossibili da rilevare, anche da parte di esperti periti grafologi; la motivazione a questa dichiarazione viene fornita negli ultimi due capitoli di questo articolo.

In terza posizione abbiamo il grande valore legale assegnato alla FEA in generale e quindi anche alla firma grafometrica; questo rende il firmatario/ utente/cittadino, estremamente vulnerabile e con criticità in caso di un contenzioso.

In ultimo, ma forse una delle cose più importanti, al contrario di un certificatore accreditato, non ci sono vincoli finanziari o assicurativi per un fornitore di FEA; questo significa che in caso di danni, nessuno sarà garantito.

Procedura operativa di una firma grafometrica

Lo scenario in cui viene introdotta una firma grafometrica, risiede tipicamente in un sistema chiuso, come ad esempio quello dell'ambiente bancario o quello di un gestore di telefonia.

L'ambito è quello di una procedura documentale, dove ad un certo momento esiste la necessità di fare apporre una o più firme autografe da parte dell'utente/cliente; il tutto anche su più copie cartacee del documento stesso.

Questi documenti, vengono poi distribuiti, in parte per i processi di archiviazione/conservazione da parte dell'azienda proprietaria della procedura documentale, in parte forniti ad altri attori del procedimento ed in ultimo, anche come ricevuta dell'evento all'utente/cliente.

In un contesto di questo tipo, sostituire la fase di firma autografa con una fase di firma grafometrica, eleva l'indice globale di efficienza del sistema, elimina i costi di produzione dei documenti cartacei ed i costi della loro successiva archiviazione e gestione nel tempo.

La postazione di lavoro su cui operare consiste tipicamente di:

- un personal computer;
- una tavoletta grafica adeguata, connessa al computer;
- un sistema di firma qualificata (da parte dell'operatore del sistema);
- un software capace di gestire li processi e le politiche di sicurezza inerenti la firma grafometrica; in genere vengono messe a disposizione delle API in modo che una procedura documentale possa integrare con facilità questa funzione;

Partendo dal presupposto che i documenti da firmare siano in formato PDF, i passi procedurali per generare una firma grafometrica che corrisponda ai requisiti indicati nella legge potrebbero essere i seguenti:

- il sw renderizza il documento da firmare[2] sullo schermo della tavoletta grafica, in modo che l'utente firmatario possa avere piena consapevolezza dell'operazione;
- sempre sulla tavoletta, l'utente si posiziona sullo speciale spazio dedicato a ricevere la sua firma autografa;
- l'utente effettua una firma autografa utilizzando la tavoletta grafica[3] e lo stilo in dotazione, quindi conferma l'operazione o la annulla per ricreare la firma ovvero abbandona definitivamente il processo di firma;
- la tavoletta trasmette i dati registrati durante l'operazione di firma, al software[4];

---

[2] primo passaggio critico; c'è da valutare l'affidabilità del sw che trasforma il file PDF originale in una renderizzazione sullo schermo della tavoletta; il sw opera una conversione in tempo reale; quello che l'utente vede non è il contenuto originale del documento

[3] l'effetto grafico sulla tavoletta e nel campo firma del documento è quello di una classica firma sulla carta: "ink effect"

[4] tramite un canale sicuro e/o dopo averli codificati; vedi paragrafo "Analisi Sicurezza del processo di firma grafometrica"

- dipendentemente dalla implementazione, il software utilizza tecniche di hashing come strumento di verifica dell'integrità dei dati e come collegamento tra i dati grafometrici ed il documento originale (PDF) da firmare;
- in tutte (?) le implementazioni, i dati grafometrici non rimangono in chiaro al termine del processo; il software li codifica con la chiave pubblica di una coppia dedicata[5] ed inserisce questa struttura in uno speciale campo-contenitore già disponibile all'interno del file PDF originale;
- il software chiede all'operatore che è stato testimone dell'operazione di firma grafometrica, di effettuare una firma qualificata del file PDF così aggiornato; la firma (PAdES) comprende naturalmente anche il/i campo/i-contenitore;

La necessità di proteggere i dati grafometrici

Tutti i produttori sono indaffarati a dimostrare che i dati grafometrici sono sempre protetti e solo davanti ad un pubblico ufficiale, tipicamente in sede di giudizio, sarebbe plausibile averli in chiaro, probabilmente allo scopo di permettere una perizia grafologica.

Quale è la ragione di questa preoccupazione che da un lato sembra aggiungere una piccola complessità al processo di creazione della firma grafometrica, ma dall'altra complica in modo significativo il processo di verifica di questa?

Sicuramente la presenza di dati biometrici, genera il timore che il Garante per la protezione dei dati personali, possa intervenire a limitare o bloccare del tutto l'uso di questo approccio, così promettente dal punto di vista dei risparmi e semplificazione dei processi documentali.

La dichiarazione che i dati biometrici saranno blindati per chiunque, a parte le Istituzioni in tempi e modi controllabili, rende il Garante sicuramente tranquillo e apre la possibilità di business.

Garante o meno, è comunque ovvio che la disponibilità dei dati grafometrici in chiaro, lascerebbe aperto il campo alla possibilità di generare *falsi autentici* da parte di operatori male intenzionati.

Ma le misure di sicurezza che vengono messe in campo, sono realmente sicure?

Naturalmente non mi riferisco ai singoli algoritmi di crittografia in campo: do per scontato che vengano utilizzati solo quelli riconosciuti come validi in ambito internazionale e naturalmente conformi alle regole tecniche in vigore.

---

[5] la coppia di chiavi asimmetriche, possibilmente nate all'interno di un SSCD è tipicamente specifica del sistema chiuso dove si sta operando; la chiave privata ovvero l'SSCD, è conservata da una terza parte di fiducia: una Certification Authority accreditata, un notaio ...

Mi riferisco piuttosto, all'intero processo composto da strumenti hw, sw e procedurali.

Le regole tecniche di (speriamo) prossima pubblicazione, cercano di governare almeno in parte, la folla di sviluppatori che si appresta a scendere in campo con soluzioni di firma grafometrica.

In particolare

> ***Art. 55 (Disposizioni generali)***
>
> *1. La realizzazione di soluzioni di firma elettronica avanzata è libera e non è soggetta ad alcuna autorizzazione preventiva.*
>
> ***Art. 58 (Soggetti che realizzano soluzioni di firma elettronica avanzata a favore di terzi)***
>
> *1. I soggetti di cui all'articolo 55, comma 2, lettera b) che offrono una soluzione di firma elettronica avanzata alle pubbliche amministrazioni, devono essere in possesso della certificazione di conformità del proprio sistema di gestione per la sicurezza delle informazioni ad essi relative, alla norma ISO/IEC 27001, rilasciata da un terzo indipendente a tal fine autorizzato secondo le norme vigenti in materia.*
>
> *2. I soggetti di cui all'articolo 55, comma 2, lettera b) che offrono soluzioni di firma elettronica avanzata alle pubbliche amministrazioni, ovvero le società che li controllano, devono essere in possesso della certificazione di conformità del proprio sistema di qualità alla norma ISO 9001 e successive modifiche o a norme equivalenti.*

Non è chiaro del perchè non si sia preteso che ambedue le certificazioni riportassero nell'oggetto in modo esplicito la voce sviluppo software, visto che questo è uno dei punti critici, ma tant'é.

In ogni caso, certificazione o meno, al momento tutta la sicurezza del processo di firma grafometrica, si basa sul fatto che un software, in esecuzione su un sistema operativo, ambedue installati su un personal computer standard, dia garanzie che il pacchetto dati proveniente dalla tavoletta grafica, non venga "spiato" da un elemento di terza parte.

Ovvero, il giorno che questo software possa essere certificato al massimo livello, tutto si baserà sul fatto che al momento della generazione della firma grafometrica, il software attivo sulla stazione di lavoro, sia effettivamente quello certificato e non uno dedicato ad intercettare in modo fraudolento i dati biometrici.

Ma anche se un giorno sia il software di gestione, sia l'intero processo di firma grafometrica, sia la stazione di lavoro dove viene svolta la procedura e la stessa tavoletta saranno certificati al massimo livello di sicurezza, dovremo iniziare a preoccuparci di cosa succede al momento in cui ci sarà la necessità di una verifica da parte di un perito grafologo.

In quel momento infatti, il pacchetto di firma grafometrica dovrà obbligatoriamente essere decodificato per permettere l'analisi da parte del grafologo:

chi certificherà l'impossibilità di effettuare una copia illecita dei dati in chiaro?

Gli strumenti forensi ed il ruolo del grafologo

ovvero (senza offesa): per prendere un ladro ce ne vuole un'altro

In ultimo, blindato anche l'ambiente di verifica forense e gli strumenti a disposizione del grafologo, messa in atto un meccanismo affidabile di Data Lost Prevention ... rimarrà sempre il fatto che da qualche parte, al di fuori del controllo di chiunque, una vittima potenziale un giorno apporrà la sua firma autografa da qualche parte, senza sapere che sotto una superficie apparentemente innocente, c'è una tavoletta grafometrica che ha catturato tutta l'informazione necessaria per produrre, non solo una sua firma, ma una serie di sue firme diverse tra loro, ma contemporaneamente uguali dal punto di vista della tecnica grafologica.

I dati relativi alle operazioni di firma, sono registrati da una tavoletta con una frequenza definita (200 elementi al secondo); ogni elemento contiene una serie di informazioni relativa alla posizione, alla pressione ed alla angolazione della penna, rispetto al piano di scrittura.

Una volta disponibili, tutti questi dati sono a disposizione del grafologo; la rappresentazione, è principalmente fatta tramite visualizzazione grafica della firma stessa, sia in modo statico che dinamico; inoltre a partire dai dati grezzi è semplice ricavare una serie di grafici in funzione dei parametri diretti o indiretti, che il grafologo utilizza proprio per valutare la firma: la posizione della penna nel tempo -anche quando questa è sollevata dalla superficie della tavoletta- la velocità di scrittura, le incertezze e le pause durante la scrittura e così via.

Tutte queste informazioni permettono ad esempio di capire se una firma è stata apposta di getto o se è stata ad esempio ricalcata da una originale.

Ma chi impedirà ad un disonesto che avesse a disposizione questi dati grezzi, di modificarli tramite opportune competenze grafometriche, allo scopo di generare in serie, false firme autentiche?

Piccole modifiche, distorsioni mirate, eliminazione delle pause illogiche in una firma autentica, renderebbero queste firme diverse tra loro, ma non ne varierebbero le caratteristiche che permettono al grafologo di accettarle come vere.

Quanto sarebbe difficile anche oggi, per un esperto grafologo, partire dal ricalco effettuato su una tavoletta grafometrica di una firma autografa, per poi cambiare i dati di comportamento così registrati, in modo che possano essere valutati da un perito grafologo come una firma autografa autentica?

L'eliminazione delle pause generate durante un ricalco, l'aumento della velocità di tracciamento etc... sono tutte modifiche che potrebbero rendere "vera" una firma falsa.

Conclusioni

Se queste riflessioni, sono anche solo in parte accettabili, l'introduzione per legge di una tecnologia di questo tipo, aprirà le porte ad infiniti, inutili e costosi contenziosi.

Inoltre l'inversione dell'onere della prova, esporrà i singoli ad una serie di possibili sopprusi, senza la minima possibilità di difesa.

Quindi, perchè affrontare questi rischi? Che necessità abbiamo di tutto questo?

Probabilmente ha invece più senso ripensare ad un'utilizzo più fluido, ma sempre controllabile, della firma qualificata basata su dispositivi sicuri, magari in modalità remota; per i vincoli a cui è soggetta, una firma qualificata è sicuramente oggi meno prona ad essere sfruttata in modalità negativa.