Sistema di misurazione e valutazione della *Performance*

Obiettivo specifico intersettoriale n. 3 – anno 2022
"*Prosecuzione del processo di digitalizzazione attraverso l'implementazione, nel sistema di gestione documentale in uso, di ulteriori tipologie di documenti afferenti alle attività dell'Ente*".

Coordinatore: Dott. Angelo Daniele Scopelliti

* * * * *

Dematerializzazione dei contratti - Approfondimento sulla possibilità di utilizzo della firma elettronica avanzata (FEA) in alternativa alla firma digitale.

1. QUADRO NORMATIVO

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.
Il recepimento della Direttiva, avvenuto con il D. lgs. 10/2002, ha comportato una notevole modifica del quadro normativo di riferimento; in particolare, l'articolo 6 del decreto di recepimento ha modificato l'articolo 10 del DPR 445/00, stabilendo che il documento informatico[1], ha l'efficacia probatoria prevista dall'articolo 2712 del codice civile[2].
Con l'entrata in vigore, nel gennaio 2006, del Codice dell'amministrazione digitale (CAD) – istituito con il decreto legislativo 7 marzo 2005, n. 82 - il valore probatorio del documento informatico ha subito un'ulteriore modifica; difatti al comma 2 dell'articolo 21 - come modificato dal D. lgs. 4 aprile 2006, n. 159 - è stabilito che "*Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile*[3]*. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria*".
Il CAD, inoltre, ha rivisto anche le tipologie di firma elettronica, prevedendone le seguenti tre:
- **la firma elettronica**, ovvero l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;

[1] Cfr. art. 1, comma 1 lett. b) del DPR 445/00: DOCUMENTO INFORMATICO la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
[2] Art. 2712 C.C. (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.
[3] Art. 2702 C.C. (Efficacia della scrittura privata).
La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa e' legalmente considerata come riconosciuta.

- **la firma elettronica qualificata**, ovvero la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;
- **la firma digitale**, ossia un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Con le modifiche al CAD - intervenute con il d.lgs. n. 235/2010 - è stata reinserita nel nostro ordinamento la **firma elettronica avanzata** (d'ora in avanti denominata **FEA**) parificandola formalmente a quella digitale; entrambe, infatti, risultano avere lo stesso valore giuridico e probatorio, ovvero quello previsto per le scritture private dal nostro codice civile, nonostante i differenti livelli di garanzia sulla provenienza e l'integrità offerti dai due sistemi di firma.

Fino al 2013, a parte una scarna definizione formale, è mancata una sostanziale regolamentazione della **FEA** 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*".

Le caratteristiche della **FEA** sono evidenziate nell'art. 26 del Regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (d'ora in avanti Regolamento eIDAS), che costituisce il quadro attuale comune di riferimento per tutti gli Stati Membri dell'Unione Europea e contiene le definizioni di firma elettronica, **firma elettronica avanzata** e firma elettronica qualificata, che si riportano di seguito:

*la **firma elettronica** rappresenta un insieme di «dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare»;*

*la **firma elettronica avanzata**, invece, deve soddisfare i requisiti di cui all'articolo 26 dello stesso Regolamento e, pertanto, deve essere «connessa unicamente al firmatario, idonea a identificare il firmatario, creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo, e collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati»;*

*l*a **firma elettronica qualificata**, infine, consiste in «*una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche».*

Un'ulteriore modifica al CAD è stata effettuata dal legislatore italiano con i decreti legislativi 179/2016 e 217/2017, che fanno espresso riferimento al citato Regolamento eIDAS.

Le differenze tra le tipologie di firma elettronica individuate a livello europeo risiedono principalmente nelle diverse modalità di identificazione del firmatario, della certificazione del contenuto firmato, della certificazione della data di firma e nella garanzia in termini di disponibilità, recupero, integrità e immodificabilità del dato.

La diretta ricaduta nella scelta del modello di firma elettronica da apporre su un documento riguarda certamente l'efficacia probatoria delle già menzionate firme in sede giudiziale; in tal senso, è bene

chiarire immediatamente che il valore probatorio delle firme elettroniche semplici è sempre liberamente interpretabile dal giudice, mentre diversa è la situazione per la firma elettronica avanzata e la firma elettronica qualificata.
La firma elettronica semplice, strumento concepito a livello comunitario soprattutto per regolamentare le transazioni commerciali tipiche dell'e-commerce, 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 tipologie di firma, invece, viene riconosciuta la medesima validità della "forma scritta e sottoscritta" anche se con molte limitazioni per la **FEA**. Ciò nonostante, quest'ultima si sta diffondendo notevolmente sul mercato.
La stessa amministrazione pubblica non è tenuta a utilizzare sempre e comunque la firma digitale ma, di volta in volta, può individuare differenti soluzioni di firma elettronica a seconda della documentazione che intende sottoscrivere o far sottoscrivere.
In effetti, anche la cosiddetta firma elettronica "semplice" può essere astrattamente idonea a far acquistare al documento informatico su cui è apposta il requisito della forma scritta e il suo valore probatorio, pur essendo questi requisiti liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità.
La firma elettronica semplice può essere, dunque, validamente utilizzata in una pubblica amministrazione per tutti gli atti interni, cioè quando il documento informatico da sottoscrivere rimane all'interno del sistema gestionale dell'ente – che ne garantisce la sicurezza informatica, e, in tal modo, anche il valore giuridico – e non necessita quindi del "sigillo di autenticità e integrità" proprio della firma digitale, richiesto invece per sottoscrivere ad esempio un documento informatico contenente un provvedimento definitivamente adottato o un atto da pubblicare sull'albo pretorio on line dell'ente o da trasmettere a un'altra pubblica amministrazione.
Alle altre tre tipologie di firma (avanzata, qualificata e digitale), invece, viene riconosciuta la medesima validità della "forma scritta e sottoscritta", anche se sono previste alcune limitazioni per l'utilizzo della **FEA**.
Ad ogni modo, la **FEA** è una firma elettronica che consente l'identificazione del firmatario, garantisce la connessione univoca con quest'ultimo, è creata con mezzi sui quali il firmatario può conservare un controllo esclusivo che gli consente di rilevare eventuali modifiche dei dati cui è apposta.
Alla luce di tale definizione, appare evidente che il Legislatore non ne ha precisato le caratteristiche tecniche, lasciando aperta la possibilità di utilizzare modalità differenti per apporre tale firma: dall'impiego di codici di identificazione personali fino all'uso di tecniche di tipo biometrico. Una firma elettronica avanzata potrà pertanto essere classificata a seconda del meccanismo di identificazione scelto e utilizzato. In generale tale firma rappresenta una modalità intuitiva per gli utenti senza i vincoli tecnologici delle firme digitali o qualificate, mantenendo un valore probatorio elevato.
Inoltre, la **FEA** consente in via digitale di conferire a un documento informatico lo stesso valore legale di una scrittura privata, semplificando di molto le attività di chi la utilizza per sottoscrivere atti e accertare la propria identità. Può, infatti, essere utilizzata da remoto e da dispositivi mobili, garantisce un alto livello di sicurezza e costituisce un valido strumento per attuare la dematerializzazione, rappresentando, così, una soluzione intermedia tra la firma elettronica semplice

e la firma elettronica qualificata. Se la prima tipologia di firma, infatti, non è in grado per le sue caratteristiche tecniche di garantire il valore legale del documento, l'altra può risultare troppo complessa per un comune utilizzo quotidiano.
Per quanto riguarda, invece, il valore giuridico dei documenti informatici con **firma elettronica avanzata**, qualificata e digitale, essi hanno la medesima efficacia probatoria ai sensi dell'art. 20, comma 1-bis del CAD ove si dispone che il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'art. 2702 del Codice civile.
L'unica eccezione riguarda la sottoscrizione degli atti di cui all'art. 1350 del Codice civile, comma 1, nn. 1-12, come quelli aventi ad oggetto beni immobili, per i quali la firma elettronica avanzata non è da ritenersi sufficiente.
La **FEA** può, pertanto, essere utilizzata per tutti i contratti stipulati dal Consiglio regionale, ad esclusione dei contratti aventi ad oggetto beni immobili e degli atti pubblici, ai sensi dell'art. 21, c. 2-bis del CAD.

2. UN PARTICOLARE TIPO DI FEA: LA FIRMA GRAFOMETRICA.

La firma grafometrica è un processo informatico che, nel rispetto di quanto previsto dal CAD, implementa un particolare tipo di firma elettronica avanzata, in grado di sostituire una tradizionale firma autografa apposta su un documento cartaceo. Realizzare una soluzione di firma grafometrica richiede l'integrazione di uno specifico software con dispositivi esterni (denominati tablet o signature pad), che consentono di acquisire la firma dell'utente. Tali strumenti sono in grado di rilevare e registrare sia dati statici (come l'immagine della firma) sia dati dinamici (fra questi l'accelerazione, la velocità, l'inclinazione, la pressione ed i movimenti aerei).
Pertanto, sul documento informatico così firmato sono conseguentemente memorizzate sia informazioni statiche sia dinamiche: l'immagine della firma viene posta in una sezione visibile, mentre i dati biometrici sono integrati nella componente informatica del documento stesso e, quindi, non sono visibili. La validazione della firma avviene direttamente in digitale, confrontando i parametri biometrici della firma con il profilo depositato. Si specifica che per dati biometrici si intende, ad esempio, la velocità di scrittura o la pressione esercitata o anche il numero di volte che lo strumento di scrittura viene sollevato nell'atto di firma.
La firma grafometrica soddisfa il requisito della connessione univoca e della identificazione certa del firmatario e del suo controllo esclusivo sullo strumento di firma.
È opportuno precisare che le firme grafometriche devono essere distinte da altre tipologie di firme realizzate con sistemi che si limitano ad acquisire solamente l'immagine della firma e non anche i dati biometrici, non memorizzando gli elementi caratteristici del tratto del firmatario. Queste firme elettroniche semplici, dunque, sono facilmente disconoscibili perché non rispondono ai requisiti fissati dall'AgID per garantire sicurezza, integrità e immodificabilità del documento e, conseguentemente, il valore probatorio dei documenti firmati con tale modalità è liberamente valutabile in giudizio.
Riguardo l'utilizzo della firma grafometrica nelle pubbliche amministrazioni, occorre rammentare la vigenza dell'art. 58 DPCM 22 febbraio 2013, ai sensi del quale:

- i soggetti di cui all'art. 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;

- i soggetti di cui all'art. 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.

Da ultimo, resta poi da considerare che, in mancanza dei suddetti requisiti, la soluzione di firma grafometrica potrà anche essere ricondotta nell'alveo della firma elettronica semplice, ovviamente con tutti i limiti probatori previsti dall'art. 20, comma 1 bis del CAD.

Occorre evidenziare che il Gruppo per la tutela dei dati personali - istituito ai sensi dell'art. 29 della direttiva 95/46/Ce - ha ritenuto che l'utilizzo di sistemi basati sull'impiego di dispositivi in grado di rilevare le caratteristiche "dinamiche" della firma determini un trattamento di dati biometrici di natura comportamentale, come tale riconducibile nell'ambito di applicazione della disciplina in materia di protezione dei dati personali[4] .

Ciò comporta che i sistemi di apposizione della predetta firma devono essere conformi alla disciplina in materia di Privacy, con particolare riferimento all'osservanza dei principi di necessità, liceità, finalità e proporzionalità.

Il Garante per la protezione dei dati personali, pertanto, in data 12 novembre 2014, ha adottato un provvedimento prescrittivo in tema di biometria, contenente nell'allegato A le "Linee Guida in materia di riconoscimento biometrico e firma biometrica".

Tale provvedimento prescrive gli obblighi che la PA deve rispettare nei confronti degli utenti, che integrano le regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali stabilite nel DPCM 22 febbraio 2013.

Allo stato gli adempimenti principali appaiono essere i seguenti:

- identificazione dell'utente in modo certo tramite un valido documento di riconoscimento e informativa in merito agli esatti termini e condizioni relative all'uso del servizio, compresa ogni eventuale limitazione dell'uso;
- subordinazione dell'attivazione del servizio alla sottoscrizione di una dichiarazione di accettazione delle condizioni del servizio da parte dell'utente (tale prescrizione è presente sia nel DPCM 22 febbraio 2013 sia nelle linee guida del Garante); a tale regime fa eccezione quanto previsto dall'art. 57, comma 5, del DPCM 22 febbraio 2013 ai sensi del quale "nell'ambito delle pubbliche amministrazioni e in quello sanitario limitatamente alla categoria di utenti rappresentata dai cittadini fruitori di prestazioni sanitarie, la dichiarazione di accettazione delle condizioni del servizio prevista al comma 1, lettera a) può essere fornita oralmente dall'utente al funzionario pubblico o all'esercente la professione sanitaria, il quale la raccoglie in un documento informatico che sottoscrive con firma elettronica qualificata o firma";
- conservazione per vent'anni del documento e della dichiarazione di accettazione del servizio, garantendone la disponibilità, integrità, leggibilità e autenticità; tale dichiarazione dovrà poter essere fornita gratuitamente, in ogni momento, a richiesta dell'interessato e dovranno essere rese note anche le modalità con le quali effettuare la predetta richiesta (mediante pubblicazione anche sul sito della pubblica amministrazione).

[4] Cfr. documento di lavoro sulla biometria del 1° agosto 2003, Wp 80; cfr. altresì Parere 3/2012 sugli sviluppi nelle tecnologie biometriche del 27 aprile 2012, WP 193.

• specificazione delle caratteristiche delle tecnologie utilizzate e pubblicazione delle caratteristiche del servizio sul proprio sito internet (meglio se in forma di nota tecnica prodotta dal fornitore del sistema).
• disponibilità, ove possibile, di un servizio di revoca del consenso all'utilizzo della soluzione di firma elettronica avanzata e un servizio di assistenza.

Ulteriori disposizioni sono contenute nel provvedimento prescrittivo del Garante, ove si prevede in particolare che:
• devono essere resi disponibili sistemi alternativi (cartacei o digitali) di sottoscrizione, che non comportino l'utilizzo di dati biometrici;
• la cancellazione dei dati biometrici grezzi e dei campioni biometrici deve aver luogo immediatamente dopo il completamento della procedura di sottoscrizione e nessun dato biometrico dovrà persistere all'esterno del documento informatico sottoscritto;
• i dati biometrici e grafometrici non devono essere conservati, neanche per periodi limitati, sui dispositivi hardware utilizzati per la raccolta, dovendo invece essere memorizzati all'interno dei documenti informatici sottoscritti in forma cifrata tramite sistemi di crittografia a chiave pubblica con dimensione della chiave adeguata alla dimensione e al ciclo di vita dei dati e certificato digitale emesso da un certificatore accreditato ai sensi dell'art. 29 del CAD;
• la corrispondente chiave privata deve essere nella esclusiva disponibilità di un soggetto terzo fiduciario che fornisca idonee garanzie di indipendenza e sicurezza nella conservazione della medesima chiave. La chiave può essere frazionata tra più soggetti ai fini di sicurezza e integrità del dato. In nessun caso il soggetto che eroga il servizio di firma grafometrica può conservare in modo completo tale chiave privata. Le modalità di generazione, consegna e conservazione delle chiavi devono essere dettagliate nell'informativa resa agli interessati;
• la trasmissione dei dati biometrici tra sistemi hardware di acquisizione, postazioni informatiche e server avviene esclusivamente tramite canali di comunicazione resi sicuri con l'ausilio di tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati;
• devono essere adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modifica della configurazione delle postazioni informatiche e dei dispositivi, se non esplicitamente autorizzati;
• i sistemi informatici sono protetti contro l'azione di malware e sono, inoltre, adottati sistemi di firewall per la protezione perimetrale della rete e contro i tentativi di accesso abusivo ai dati;
• nel caso di utilizzo di sistemi di firma grafometrica nello scenario mobile o BYOD (Bring Your Own Device), sono adottati idonei sistemi di gestione delle applicazioni o dei dispositivi mobili, con il ricorso a strumenti MDM (Mobile Device Management) o MAM (Mobile Application Management) o altri equivalenti al fine di isolare l'area di memoria dedicata all'applicazione biometrica;
• devono essere ridotti i rischi di installazione abusiva di software anche nel caso di modifica della configurazione dei dispositivi e contrastare l'azione di eventuali agenti malevoli (malware);
• i sistemi di gestione impiegati nei trattamenti grafometrici adottano certificazioni digitali e politiche di sicurezza che disciplinino, sulla base di criteri predeterminati, le condizioni di loro utilizzo sicuro

(in particolare, rendendo disponibili funzionalità di remote wiping applicabili nei casi di smarrimento o sottrazione dei dispositivi);

- l'accesso al modello grafometrico cifrato deve avvenire esclusivamente tramite l'utilizzo della chiave privata detenuta dal soggetto terzo fiduciario, o da più soggetti, in caso di frazionamento della chiave stessa, e nei soli casi in cui si renda indispensabile per l'insorgenza di un contenzioso sull'autenticità della firma e a seguito di richiesta dell'autorità giudiziaria.

Il successivo documento del Garante per la Protezione dei dati personali recante 'Sistema di firma elettronica avanzata grafometrica. Verifica preliminare' del 4 giugno 2015, ribadisce che, sotto il profilo della sicurezza dei dati trattati, i sistemi di apposizione della summenzionata firma devono essere conformi a quanto previsto nel paragrafo 4.4. del Provvedimento generale del Garante in materia di biometria del 12 novembre 2014, con particolare riguardo alle caratteristiche tecniche e alle prescrizioni ivi individuate, ad esclusione di quanto previsto dalla lettera d), relativamente alla previsione di utilizzare, ai fini della cifratura dei dati biometrici, un certificato digitale emesso da un certificatore accreditato ai sensi dell´art. 29 del Codice dell'amministrazione digitale.
Il medesimo provvedimento ribadisce altresì che occorre:
- fornire agli interessati, tra l'altro, le indicazioni relative alle caratteristiche del sistema proposto, mettendo in rilievo la possibilità, per coloro che non intendano autorizzare l'utilizzo dei dati biometrici nell'ambito della prospettata soluzione, di avvalersi delle tradizionali modalità di autenticazione;
– conservare i dati biometrici dei firmatari per il solo periodo di tempo strettamente necessario al perseguimento degli scopi per i quali gli stessi sono stati raccolti e successivamente trattati, salva la possibilità di un'ulteriore conservazione in ragione di specifiche previsioni normative o della tutela di eventuali diritti in sede giudiziaria;
– non utilizzare i dati biometrici dei firmatari in operazioni di trattamento non compatibili con le finalità originarie della raccolta.

Riguardo i rapporti giuridici per i quali può essere utilizzata una soluzione di firma grafometrica, l'art. 60 del DPCM 22 febbraio 2013, stabilisce che "*La firma elettronica avanzata realizzata in conformità con le disposizioni delle presenti regole tecniche, è utilizzabile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore e il soggetto di cui all'art. 55, comma 2, lettera a)*".
In virtù di tale norma regolamentare, l'utilizzo di un procedimento di FEA farà sì che le sottoscrizioni apposte con l'utilizzo della firma grafometrica possano esplicare la loro efficacia esclusivamente nell'ambito dei rapporti tra il cittadino e la pubblica amministrazione erogatrice del servizio, esclusa ogni ipotesi di ultrattività e diversa valenza giuridica della firma.
Stante le numerose prescrizioni sull'utilizzo della firma grafometrica, appare utile qualche considerazione sulle conseguenze del mancato rispetto delle norme che disciplinano l'erogazione di un servizio di firma grafometrica, per il quale si possono ipotizzare due rischi potenziali:

- un più agevole disconoscimento delle firme da parte del cittadino che impegnerebbe la pubblica amministrazione in lunghi ed estenuanti processi di verificazione dell'autenticità delle firme stesse ovvero in altrettanto lunghi processi conseguenti a querela di falso;
- l'eccezione del cittadino o dell'utente professionale (impresa/professionista) volta a sostenere che la soluzione di firma grafometrica proposta non sarebbe conforme alle regole tecniche di cui al DPCM 22 febbraio 2013 e dunque non potrebbe essere ricondotta nell'alveo della firma elettronica avanzata.

Ove accolta, una tale eccezione, comporterebbe una rilevante perdita del valore giuridico delle firme apposte, potendo le stesse essere degradate al livello di firme elettroniche semplici, con la conseguenza che il documento, non più assistito dall'efficacia di cui all'art. 2702 del Codice civile, sarebbe invece liberamente valutabile dal giudice, venendo in sostanza parificato ad una normale e-mail.

3. IN QUALI CONTESTI OPERATIVI È APPLICABILE LA FIRMA GRAFOMETRICA.

Per come disciplinata nel DPCM 22 febbraio 2013, la firma grafometrica non è un semplice metodo di sottoscrizione di documenti informatici, ma un vero e proprio processo che serve a garantire, a seconda del contesto, un certo grado di validità giuridica ed efficacia probatoria in tutto il ciclo di vita del documento amministrativo informatico che comprende le fasi di formazione, gestione, conservazione, esibizione e scarto del documento. Nell'adozione di una soluzione di firma grafometrica vanno individuati, pertanto, gli impatti operativi in ciascuna delle predette fasi del ciclo di vita del documento e per tal motivo è ancor più raccomandabile adottare in questi progetti un approccio "per processo".
La firma grafometrica, pertanto, **necessità di requisiti e condizioni di contesto che la rendono meno agile di altri strumenti di firma**.
Semmai, il contesto ideale per massimizzarne i vantaggi pratici riguarda le attività di sportello a contatto diretto con l'utenza che prevedono la sottoscrizione di documenti informatici in presenza del funzionario addetto e in tempo reale rispetto alla produzione del documento; in questo contesto, infatti, l'utente può firmare validamente un documento informatico con uno strumento a lui familiare (la penna) e secondo modalità (la firma autografa) che non richiedono specifiche competenze tecniche, né l'utilizzo di dispositivi particolari o codici di accesso.
Sebbene possa essere utilizzata per tutti i contratti stipulati dalla pubblica amministrazione (ad esclusione dei contratti aventi ad oggetto beni immobili e degli atti pubblici), la firma grafometrica può essere validamente utilizzata per la **sottoscrizione di istanze e dichiarazioni**, atteso che secondo l'art. 20, c. 1 bis del CAD, il documento informatico sottoscritto con firma elettronica avanzata, ha l'efficacia prevista dall'articolo 2702 del Codice civile.
Trattandosi di documenti (amministrativi) informatici e dovendone garantire l'integrità e l'immodificabilità è necessario fare riferimento alle regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici, nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni, contenute nelle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" di AGID.
Poiché la caratteristica principale del documento informatico è rappresentata proprio dalla sua immodificabilità, il documento deve quindi essere prodotto in modo da garantirne l'inalterabilità della forma e del contenuto durante le fasi di gestione e tenuta, nonché la staticità in fase di conservazione.
A tal fine, il documento informatico deve essere prodotto in uno dei formati di file contenuti nell'allegato 2 ("Formati di file e riversamento") alle predette Linee Guida, in modo da assicurarne l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra sistemi informatici e la durata nel tempo in termini di accesso e di leggibilità. Formati diversi possono essere scelti e utilizzati nei casi in cui la natura del documento informatico lo richieda per il suo utilizzo in un contesto specifico; in

tal caso, tuttavia, gli eventuali ulteriori formati devono essere esplicitati, motivati e riportati nel manuale di gestione.

In merito alle modalità di trattamento dei dati, occorre precisare che i documenti informatici sottoscritti con firma grafometrica - al pari di tutti gli altri documenti amministrativi (informatici e non) prodotti o acquisiti dalla PA - devono confluire nel sistema di gestione informatica dei documenti di cui al DPR 445/2000 per essere registrati, classificati, assegnati agli uffici di competenza e fascicolati a cura di questi ultimi. Qualora il sistema che gestisce il processo di formazione e sottoscrizione dei documenti con firma grafometrica sia diverso dal software di gestione documentale, come spesso accade, è necessario prevedere l'integrazione dei due sistemi in modo che i documenti, una volta prodotti e firmati, confluiscano per effetto di procedure automatizzate nel sistema di gestione dei documenti, all'interno del quale saranno trattati secondo le regole e le prassi archivistiche descritte nel manuale di gestione.
La registrazione dei documenti informatici sottoscritti con firma grafometrica può avvenire secondo una delle modalità previste dal DPR 445/2000 e quindi all'interno del registro di protocollo o di specifici repertori quale forma di registrazione particolare di determinate tipologie documentarie. Qualora i documenti siano già soggetti ad una forma di registrazione nell'ambito dell'applicativo in cui sono stati prodotti e sottoscritti, purché tale forma di registrazione sia descritta nel manuale di gestione, i documenti possono essere importati nel sistema di gestione informatica dei documenti e inseriti in appositi registri di documenti non protocollati, né soggetti ad altra forma di registrazione (repertorio). L'integrazione tra il sistema (o i sistemi) di produzione e sottoscrizione dei documenti informatici con firma grafometrica e il sistema di gestione informatica dei documenti è fondamentale anche ai fini della conservazione secondo quanto previsto dalle regole tecniche di cui al DPCM 3 dicembre 2013.

4. CONSIDERAZIONI FINALI SUL POSSIBILE UTILIZZO DELLA FIRMA GRAFOMETRICA PRESSO IL CONSIGLIO REGIONALE.

Pur presentando numerosi vantaggi, la firma grafometrica, tuttavia, comporta l'osservanza di obblighi ineludibili che aggravano le attività da porre in essere in capo alla P.A., soprattutto in termini di rispetto della normativa sul trattamento dei dati personali.
Infatti, sul titolare, o sul responsabile del trattamento, gravano, in linea di massima, i seguenti obblighi:

- fornire al firmatario un'apposita informativa che illustri le caratteristiche della specifica modalità operativa, i criteri di crittografazione dei dati e le altre informazioni proprie dell'informativa privacy;
- acquisire il consenso dell'interessato all'utilizzo del sistema di firma grafometrica con il rischio, in caso di mancato consenso, che la firma non potrà che essere acquisita in modalità analogica comportando l'apposizione di firma su documento cartaceo e vanificando, in tal modo, il fine di dematerializzazione cui è tenuta la P.A.;
- evitare la persistenza di dati biometrici all'esterno del documento sottoscritto mediante firma grafometrica;
- garantire l'immediata cancellazione di dati grezzi e campioni appartenenti al firmatario subito dopo la sottoscrizione;

- non salvare i dati grafometrici all'interno dell'hardware utilizzato dall'interessato per apporre la firma e, nel contempo, accertare che i dati stessi abbiano caratteristiche di crittografia sufficientemente solida per l'ancoraggio al documento da sottoscrivere attraverso un sistema di chiavi pubblica e privata e un certificato di firma (Certification Authority – verifica dell'identità fornite per mettere in atto le misure anticontraffazione).

Inoltre, occorre procedere alla identificazione del firmatario tramite generalità, codice fiscale, oltre che attraverso un valido documento di riconoscimento. Naturalmente tutti questi dati saranno anch'essi oggetto di conservazione digitale insieme al consenso prestato all'utilizzo dello strumento informatico.

Alla luce dei numerosi adempimenti a cui sarebbe tenuto il Consiglio regionale qualora adottasse la firma grafometrica, anche in considerazione delle implicazioni sulla privacy e con il rischio che l'utente non presti il consenso al trattamento dei dati biometrici, non appare conveniente l'adozione di tale strumento all'interno dell'Amministrazione consiliare.

5. FIRMA ELETTRONICA AVANZATA TRAMITE OTP.

Nell'ambito della **FEA**, cioè della firma elettronica avanzata, rientra, altresì, quella apposta tramite OTP, acronimo che sta per "*One Time Password",* ovvero "password valida solo una volta".

Nello specifico, tale firma elettronica si basa sulla generazione di una password temporanea ricevuta via apposite App o via SMS sul proprio telefono oppure tramite Server di Messaggio vocale o nel corpo di una mail.

Il codice ricevuto tramite SMS o App sul proprio smartphone oppure sulla mail o tramite server vocale, può essere composto da 4 o più cifre e sarà valido solamente per una singola sessione di firma nel momento in cui viene generato ed inserito.

Il codice ha una validità di tempo limitata, di solito qualche minuto, e dovrà essere inserito nell'apposita casella durante la firma di un documento ed utilizzato nel tempo limite per evitare che scada e se ne debba richiedere uno nuovo. Se su uno stesso documento sono presenti più caselle di firma a nome della stessa persona, è sufficiente inserire un solo codice per apporre la firma.

Tale modalità di firma si struttura sempre come un processo finalizzato a garantire un certo grado di validità giuridica ed efficacia probatoria, che si innesta all'interno del ciclo di vita del documento nativo digitale.

Infatti, l'utilizzo del codice OTP per la firma elettronica dei documenti, sfrutta la sicurezza di un sistema di autenticazione a due fattori (Two-factor Authentication o 2FA), utilizzato ormai nella grande maggioranza dei servizi di firma per verificare l'identità dell'utente.

Da quanto riscontrato a livello operativo, l'autenticazione a due fattori è una metodologia molto semplice che viene utilizzata per confermare l'identità di un utente. Più precisamente, dopo aver inserito la password (detta anche primo fattore), necessaria per accedere al proprio account (o dopo aver cliccato sul link della procedura di firma ottenuto via email), occorre digitare o inserire il secondo fattore (codice numerico).

Il secondo fattore può essere ottenuto dall'utilizzatore in vari modi, di cui il più comune è la ricezione tramite SMS, anche se si possono utilizzare applicazioni dedicate o token hardware fisici.

Tuttavia, tale tipologia di firma, per poter rientrare a pieno titolo all'interno della FEA, necessita principalmente che il firmatario sia stato identificato in modo certo e che vi sia stata da parte sua l'accettazione delle condizioni di tale utilizzo.

Questo tipo di firma viene per lo più utilizzata nell'ambito assicurativo e bancario, per quei tipi di documenti che necessitano di un'identificazione forte del firmatario e di una maggior protezione in caso di controversia.
In tal senso, come specificato dal Regolamento dell'Unione Europea numero 910/2014, cosiddetto regolamento "eIDAS", nonché dal CAD - Codice dell'Amministrazione Digitale (D.lgs. n. 82/2005), una firma elettronica con codice OTP ha valore legale se il documento viene sottoscritto nel rispetto delle caratteristiche tecniche che garantiscano l'identificabilità dell'autore, l'integrità e l'impossibilità di modifica del documento stesso.
Inoltre, anche le soluzioni di firma elettronica avanzata, apposta tramite OTP, devono essere conformi a quanto sancito, in particolare, dalle norme di cui agli artt. 55-61 delle c.d. "*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",* di cui al DPCM 22 febbraio 2013.
Tutto ciò considerato, i vantaggi che la firma OTP presenta, rispetto alla firma grafometrica, sono tangibili:

- sono eliminati i rischi relativi all'utilizzo delle password statiche;
- le password temporanee non sono vulnerabili agli attacchi con replica;
- facilità d'uso visto che l'identificazione avviene tramite SMS (o servizi simili) contenente la password temporanea;
- mentre con la firma grafometrica bisogna essere in presenza, con l'OTP non è richiesta né la presenza, né la tavoletta grafica.

Tanto premesso, per il Consiglio regionale appare percorribile, in termini di convenienza, l'utilizzo della firma tramite OTP per la sottoscrizione dei contratti in formato digitale anche da remoto, o di qualsiasi altro documento amministrativo richiedente l'apposizione di firma da parte di chi sia sprovvisto di firma digitale.

6. **Requisiti per l'utilizzo della FEA OTP nel contesto tecnologico/organizzativo del Consiglio regionale della Calabria**.

Sarebbe necessario che l'Ente si doti di una soluzione applicativa che implementi quantomeno le funzionalità necessarie allo svolgimento alle attività di seguito elencate:

1. ***Attività di gestione del processo di firma***:
   1.1. Interfaccia verso l'operatore dell'Ente:
      1.1.1. gestione di una anagrafica degli utenti del servizio di firma, generazione e gestione dei certificati di firma;
      1.1.2. gestione del processo di firma:
      - caricamento del documento da sottoporre a firma;
      - gestione di parametri aggiuntivi (es. termine entro il quale la firma può essere apposta),;
      - monitoraggio dello stato del processo;
      - invio promemoria;
      - accesso al documento firmato.

1.2. Interfaccia verso il soggetto che firma il documento:
- visualizzazione del documento prima della firma (presa visione);
- invio del codice OTP (generalmente tramite il servizio SMS);
- generazione del documento firmato e rilascio di una copia al firmatario (generalmente tramite il servizio di posta elettronica).

1.3. Interfaccia verso il sistema di gestione documentale:
scambio dei documenti da firmare/firmati con il sistema di gestione documentale.

2. ***Attività di archiviazione e conservazione*** in conformità alla vigente normativa dei documenti informatici sottoscritti con la soluzione FEA, dei moduli di adesione/revoca e dei documenti di identità dei firmatari.

Le attività relative al punto 2 trovano implementazione nel sistema di gestione documentale già in uso presso il Consiglio regionale.

Quanto alle attività relative al punto 1:

A. La soluzione ottimale consiste nella progettazione di una versione evoluta del sistema di gestione documentale già in uso, che integri le funzionalità richieste. A tal proposito si evidenzia che, qualora dopo l'aggiornamento del software persistessero le ragioni di sicurezza che sconsigliano l'esposizione del servizio sulla rete Internet, sarà necessario prevedere un servizio dedicato, che isoli e renda disponibile all'esterno della rete informatica del Consiglio i soli documenti da firmare, minimizzando in tal modo le conseguenze di un eventuale attacco informatico.

B. Una soluzione intermedia dal punto di vista dell'automazione del processo consiste nell'acquisto di una soluzione personalizzata per l'erogazione del servizio di firma elettronica avanzata che integri, in aggiunta alle funzionalità di base (punti 1.1 e 1.2), i servizi necessari allo scambio di file con il sistema di gestione documentale (punto 1.3). L'interoperabilità tra i due sistemi sarà in tal caso basata sui "Product Integration Services" esposti dal sistema di gestione documentale.

C. In ultima analisi, l'Ente può procedere in tempi rapidi all'acquisto di una soluzione standard per l'erogazione del servizio base di firma elettronica avanzata (punti 1.1 e 1.2). Questa scelta ha lo svantaggio di gravare l'operatore di tutto l'onere relativo al trasferimento dei file da firmare/firmati tra il sistema di firma e quello di gestione documentale.

7. FIRMA ELETTRONICA AVANZATA TRAMITE CIE E CNS.

Come, d'altronde, previsto dall'art. 61, comma 2 del "*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",* di cui al DPCM 22 febbraio 2013, la Carta di identità Elettronica (CIE) e la TS-Carta Nazionale dei Servizi (CNS) rilasciate dallo Stato italiano, possono essere utilizzate come dispositivo per la firma elettronica avanzata (FEA), in quanto consentono di firmare documenti elettronici di qualsiasi tipologia.
La firma elettronica avanzata apposta con la TS-CNS o la CIE ha alti livelli di sicurezza perché:

- è generata con uno strumento (*smart card*) certificato secondo gli stessi standard di sicurezza adottati dalle *smart card* per la firma digitale (ISO/IEC 15408, Common Criteria, EAL4+);
- il certificato digitale e le chiavi sono generate da un certificatore accreditato da AgID.

Per il Consiglio regionale, appare possibile, quindi, consentire l'utilizzo della CIE o della TS-CNS per la sottoscrizione dei contratti in formato digitale, o di qualsiasi altro documento amministrativo richiedente l'apposizione di firma da parte di chi sia sprovvisto di firma digitale.