La firma elettronica. Quale valore legale?

Giovanni Gregorio
Avvocato civilista
Patrocinante in Cassazione

La firma elettronica è uno strumento che usiamo quotidianamente per la nostra attività lavorativa. Ogni giorno, inviamo e-mail e messaggi istantanei, facciamo pagamenti on-line e stipuliamo contratti contenuti in documenti informatici.

Le aziende effettuano acquisti con documenti "dematerializzati". Gli ordini, le conferme d'ordine, i contratti quadro e le condizioni generali di contratto non sono più scritti su documenti cartacei firmati a mano, ma sono ormai contenuti in documenti informatici sottoscritti elettronicamente. Ad esempio, le e-mail che i buyer inviano ai fornitori sono documenti informatici dotati di firma elettronica; ma qual è la loro efficacia giuridica? Più in generale, quale efficacia può avere un documento informatico sottoscritto con firma elettronica?

Per rispondere a queste domande bisogna innanzitutto esaminare la funzione e l'efficacia di un documento scritto e della sua sottoscrizione.

Il documento scritto e la sottoscrizione

Un qualsiasi documento scritto che riporta le dichiarazioni di un soggetto (ad es., una lettera o un contratto) acquista efficacia giuridica grazie alla firma (o sottoscrizione) del suo autore, che viene posta a chiusura del documento medesimo. L'autore di un documento cartaceo appone la propria sottoscrizione, scrivendo a mano il proprio nome e cognome. Questa sottoscrizione, basata sulla grafia e sul gesto umano, è definita firma autografa.

Quest'ultima serve, innanzitutto, per individuare l'autore del documento e costituisce la prova che quest'ultimo proviene dal soggetto che ha scritto il proprio nome e cognome. In questo modo, il firmatario si assume la paternità delle dichiarazioni contenute nel documento, facendole proprie. La firma serve, quindi, non solo a individuare l'autore del documento, ma anche a obbligarlo a fare ciò che ha dichiarato.

Quando le dichiarazioni di un soggetto sono riportate in un documento informatico (ad es., un'e-mail) quest'ultimo può contenere una firma elettronica, che ha le medesime funzioni sopra descritte per la firma autografa.

Tuttavia, mentre la firma autografa è unica, in quanto è basata sulla grafia del suo autore, le firme elettroniche possono essere di diverso tipo a seconda della procedura tecnologica utilizzata. Ognuna di esse può, quindi, avere un'efficacia giuridica diversa dalle altre.

Prima di addentrarci nei diversi tipi di firme elettroniche, bisogna fare alcuni cenni sul documento informatico.

Il documento informatico

In Italia, il Codice dell'Amministrazione Digitale (CAD) definisce **il documento informatico** come *"il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti"* (art. 1, lett. p del D.Lgs n. 82/2005).

A livello europeo, il Regolamento eIDAS (Regolamento UE n. 910/2014) definisce, a sua volta, il documento elettronico come *"qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva"* (art. 3, n. 35).

In linea generale, nella pratica, gli esempi più comuni di documenti informatici/elettronici sono: le e-mail; i documenti di testo e i fogli di calcolo; le foto, i video e gli audio digitali; i c.d. file di log; le pagine web; i messaggi istantanei (SMS, WhatsApp, Telegram, ecc...).

Come un qualunque documento sottoscritto, un documento informatico provvisto di firma elettronica acquisisce efficacia vincolante per il suo autore. Come detto, però, la sua efficacia può variare a seconda del tipo di firma elettronica associata al documento.

Vediamo, quindi, i diversi tipi di firme elettroniche previste dal nostro ordinamento.

Le firme elettroniche

Vi sono quattro diversi tipi di firma elettronica, di seguito elencati in ordine crescente in base al loro livello di sicurezza ed affidabilità:

- **la firma elettronica semplice;**
- **la firma elettronica avanzata (FEA);**
- **la firma elettronica qualificata (FEQ);**
- **la firma digitale**.

La firma elettronica semplice

La firma elettronica c.d. semplice (o "debole") è definita dall'art. 3, n. 10 del Regolamento eIDAS come un insieme di *"dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare".*

Le firme elettroniche semplici più comuni sono la *username* e la *password* o il *PIN*. Esse vengono solitamente utilizzate in combinazione tra loro come credenziali di accesso e di autenticazione a un "account" che il fornitore di un servizio mette a disposizione dell'utente per utilizzare il servizio medesimo. Ad esempio, per inviare e ricevere messaggi di posta elettronica ordinaria, l'utente deve, innanzitutto, attivare un account di posta.

Per l'attivazione, egli deve seguire una procedura di registrazione durante la quale deve inserire i propri dati e creare una *username* e una *password*, quest'ultima nota soltanto a lui. In questo modo la *username* e la *password* sono associate in modo univoco al suo account. Nelle sessioni successive, l'utente, per inviare e ricevere messaggi con il proprio account, deve preventivamente autenticarsi, inserendo la propria *username* e la propria *password.* In questo modo, i messaggi di posta elettronica inviati dal suo account risultano da lui firmati elettronicamente.

Attraverso uno scambio di e-mail è, quindi, possibile concludere un accordo giuridicamente vincolante; è possibile, cioè, stipulare un contratto.

Dei quattro tipi firma elettronica, tuttavia, quella c.d. semplice è quella meno sicura e affidabile di tutte. Essa, infatti, presenta diversi elementi di incertezza circa la sua autenticità. Innanzitutto, questo tipo di firma non prevede l'identificazione certa del firmatario. Ad esempio, durante la procedura di registrazione a un servizio di posta elettronica ordinaria, non viene chiesto all'utente di identificarsi con un documento di identità; di conseguenza, un soggetto potrebbe registrarsi fornendo false credenziali.

In secondo luogo, la firma elettronica semplice è connessa univocamente al firmatario soltanto da un'associazione logica (*username* e *password*). Ciò significa che chiunque entri in possesso della *password*, potrebbe utilizzare la firma elettronica ad essa collegata.

Da ultimo, la firma elettronica semplice, oltre a non essere assistita da un sistema di generazione sicuro, non consente di verificare che il documento informatico non abbia subito modifiche dopo l'apposizione della firma.

Per tali motivi, un'e-mail ordinaria potrebbe essere facilmente oggetto di contestazioni sulla sua effettiva provenienza. Ciò potrebbe avere conseguenze sulla sua validità ed efficacia giuridica. Prima di stipulare un contratto con tali modalità, bisogna quindi tenere conto dei rischi che ciò comporta.

La firma elettronica avanzata (FEA)

La firma elettronica avanzata (FEA) offre maggiori garanzie di sicurezza e affidabilità rispetto quella semplice, in quanto, ai sensi degli artt. 3, n. 11 e 26 del Regolamento eIDAS, essa soddisfa "*i seguenti requisiti:*

1. *è connessa unicamente al firmatario;*
2. *è idonea a identificare il firmatario;*
3. *è 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*
4. *è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati."*

Come si vede, la firma elettronica avanzata, a differenza di quella semplice, consente di identificare in modo univoco e sicuro il firmatario. Nel caso in cui il documento venisse modificato dopo l'apposizione della firma, essa consentirebbe, inoltre, di individuare ogni successiva modifica.

Esempi di firme elettroniche avanzate sono la firma grafometrica sul *tablet* della banca e la firma tramite SPID (Sistema Pubblico d'Identità Digitale).

La firma elettronica qualificata (FEQ)

Ai sensi dell'art. 3, n. 12 del Regolamento eIDAS, **la firma elettronica qualificata,** è 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".* In altre parole, la firma elettronica qualificata ha le medesime caratteristiche di una firma elettronica avanzata con l'aggiunta di due ulteriori elementi che le attribuiscono maggiore affidabilità.

Innanzitutto, essa può essere apposta soltanto con l'utilizzo di un dispositivo sicuro, tecnicamente idoneo a creare tale firma. Tale dispositivo può essere fisico oppure contenuto virtualmente in un altro dispositivo in possesso del firmatario. Esempi di dispositivi per creare una FEQ sono la *smart card*, il c.d. token (ad es. per l'utilizzo dell'home banking), un software o un'applicazione installata sullo *smartphone*.

In secondo luogo, oltre ad essere creata con tali dispositivi, la FEQ si basa su un certificato di firma qualificato rilasciato da un soggetto terzo accreditato. Il certificato qualificato è un attestato elettronico che collega i dati di convalida di una firma elettronica ad una determinata persona fisica e conferma il nome e il cognome del firmatario.

Rispetto alla firma elettronica avanzata, quella qualificata ha quindi un grado di sicurezza maggiore, in quanto consente di identificare in modo ancora più attendibile l'autore del documento.

La firma digitale

Da ultimo, il tipo di firma elettronica attualmente più sicura è **la firma digitale**. Ai sensi dell'art. 1, lett. s) del CAD, essa è *"un particolare tipo di firma qualificata, **basata su un sistema di chiavi crittografiche**, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico".*

La firma digitale, pertanto, oltre ad avere tutte le caratteristiche della firma qualificata, ha un ulteriore elemento di sicurezza in più rispetto a quest'ultima, in quanto si basa su un sistema crittografico a chiavi asimmetriche:

- una chiave "privata", conosciuta soltanto da colui che firma il documento;
- una chiave "pubblica", che consente di risalire con sicurezza al nominativo del titolare della chiave privata e di verificare l'integrità del documento informatico.

In tal modo, la firma digitale consente di verificare con un elevato grado di certezza sia la provenienza del documento informatico, sia l'integrità del suo contenuto.

Un documento informatico sottoscritto con firma digitale sarà difficilmente contestabile.

In conclusione, per la stipulazione di contratti o l'invio di comunicazioni di particolare importanza sarà opportuno utilizzare una firma digitale o, quantomeno, una firma elettronica avanzata o qualificata. Diversamente, le comunicazioni di ordinaria amministrazione possono essere effettuate mediante documenti informatici sottoscritti con firma elettronica semplice.