IL BIAS DELL'ESTENSIONE E LA FIRMA DIGITALE

di MASSIMO EROLI

Di recente la Cassazione penale[1] ha affrontato una serie di casi nei quali era stata messa in dubbio la presenza della firma digitale, che come è noto ai sensi della lettera s) del primo comma dell'art. 1 del d.lgs. 7 marzo 2005 n. 82 (codice dell'amministrazione digitale) è un particolare tipo di firma elettronica qualificata[2] 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.

Da ultimo si trattava della ritenuta, da parte del giudice del merito, inammissibilità di un appello, trasmesso attraverso pec,

[1] Le modalità di deposito degli atti ed i controlli automatici da tempo implementati nel software del processo telematico civile rendono difficile, anche se non impossibile, che simili casi si verifichino in sede civile ma il problema della verifica delle firme digitali in generale è comunque presente anche nel procedimento civile e spesso sottovalutato.

[2] La firma elettronica qualificata è, secondo ora le disposizioni del Regolamento UE n. 910/2014 tra cui gli artt. 3 e 26, quella firma che oltre alla garanzia univoca di connessione al firmatario, alla creazione con mezzi di cui il firmatario può conservare un controllo esclusivo con un elevato livello di sicurezza e al collegamento ai dati a cui la firma si riferisce che consente di rilevare se i dati siano stati modificati successivamente all'apposizione della firma (elementi propri della firma elettronica avanzata) ha anche gli altri due ulteriori elementi costituiti dall'utilizzo di un certificato qualificato di firma e dall'utilizzo di un dispositivo sicuro di firma.

per la pretesa mancanza di firma digitale del difensore. Al proposito la Cassazione[3] ha ritenuto testualmente: "*può affermarsi, in via generale, che, ai fini della verifica della sussistenza della firma digitale di un atto di impugnazione, non sussiste la necessità di ulteriori accertamenti qualora risulti in atti che il file abbia estensione pdf.p7m"* ed in altra sentenza dello stesso anno aggiunto "*posto che questa è, di per sé, provante dell'avvenuta firma digitale*"[4]. Ciò richiamando altre pronunce precedenti e specificamente quella che, però con una esposizione più ampia, l'anno prima[5] aveva affermato tra l'altro che "*la verifica di esistenza e validità della firma digitale può infatti essere effettuata solo con gli appositi software di firma (Dike, Firma Certa, Firma Ok Gold etc.) o attraverso il software ministeriale. O, in casi come quello che ci occupa, può essere insita nell'estensione stessa del file. Nel caso in esame, infatti, come si evince dalla pec dell'Avv. …, difensore del A.A., alla stessa venne allegato il ricorso sia con estensione .pdf che con estensione.pdf.p7m. Orbene, come si è detto in precedenza, un file pdf.p7m altro non è che un file firmato digitalmente, che può essere un documento di testo, un foglio elettronico, un'immagine, una fattura elettronica o un qualunque altro tipo di documento informatico sul quale, tramite un procedimento elettronico, sia stata apposta una firma digitale. Può dunque affermarsi, in via generale, che, ai fini della verifica della sussistenza della firma digitale di un atto di impugnazione, non sussiste la necessità di ulteriori accertamenti qualora risulti in atti che il file abbia estensione pdf.p7m in quanto tale estensione è essa stessa probante dell'avvenuta firma digitale dell'atto.*"

Ed ancora prima la Cassazione[6] aveva affermato che "*dalla copia della mail inviata - consultabile in considerazione della natura processuale dell'eccezione - risulta che effettivamente il file inviato aveva l'estensione ".p7m" che contraddistingue i file*

[3] Cass. pen. 37463/2024.

[4] Cass. pen. 2389/2024.

[5] Cass. pen. 43976/2023.

[6] Cass. pen. 19273/2022.

con firma digitale "CAdES". La giurisprudenza civile, che per prima è stata investita di tali tematiche, ha chiarito che in tema di processo telematico, a norma dell'art. 12 del decreto dirigenziale del 16 aprile 2014, di cui al D.M. n. 44 del 2011, art. 34, - Ministero della Giustizia -, in conformità agli standard previsti dal Regolamento UE n. 910 del 2014 ed alla relativa decisione di esecuzione n. 1506 del 2015, le firme digitali di tipo "CAdES" e di tipo "PAdES" sono entrambe ammesse e equivalenti, sia pure con le differenti estensioni ".p7m" e ".pdf" (Cass. civ., Sez.U, n. 10266 del 27/4/2018, Rv. 648132). Analogo principio va affermato anche nell'ambito del giudizio penale, posto che lo strumento informativo soggiace alla medesima disciplina, sicché deve affermarsi il principio secondo cui il file, inviato mediante posta elettronica certificata, avente estensione ".p7m" deve ritenersi sottoscritto con firma digitale".

Dalla lettura di queste parti di motivazioni è evidente come dal formato della firma digitale e del relativo documento firmato, che è una cosa, ci si sia spostati alla estensione del file, che è altra cosa, determinandosi così un vero e proprio *bias*. Non è infatti vero che se un file abbia l'estensione .p7m esso contenga una firma digitale, mentre le affermazioni della Cassazione sopra riportate e che purtroppo sono state recepite acriticamente nella loro divulgazione, specie nel web e su alcuni media "tecnici", farebbero supporre il contrario !

Da un iniziale scetticismo verso il documento informatico e le firme elettroniche, ormai superato normativamente dal principio di non discriminazione contenuto nel Regolamento europeo eIDAS[7], si è passati ad una sorta di fideismo accentuato dalla necessità di utilizzare procedure automatiche, proprie dell'informatica, verso cui però va sempre mantenuto uno spirito

[7] Primo comma art. 25 Regolamento UE n. 910/2014 per cui "*a una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate*" e primo comma art. 46 dello stesso per cui "*a un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica*".

critico e soprattutto oggi il giurista non può più ignorare quella che è l'alfabetizzazione di base dell'informatica, a causa dell'importanza assunta da quest'ultima nella realtà[8].

Stante la struttura di base degli elaboratori elettronici che ragionano in base ad una logica binaria, un documento informatico o *file* altro non è che un insieme di bit (0 o 1), a loro volta, per mera comodità, raggruppati in byte (unità di 8 bit).

Di conseguenza le informazioni in esso contenute, quale che sia la loro natura, testo, immagine, suono o altro, devono preliminarmente, attraverso l'uso di appositi programmi eseguibili, essere codificate[9] o meglio digitalizzate in base a dati algoritmi che ne determinano il formato ed in base a detti algoritmi decodificate e rese in un formato a video o a stampa o altro modo, comprensibile ad un essere umano.

Come è verificabile aprendo un qualsiasi file con programmi, ad esempio XVI32 od altro editor esadecimale, che ne mostrino il contenuto byte per byte[10] non solo gli odierni documenti informatici contengono, codificato, il loro contenuto rilevante, ma anche altre informazioni e non solo di formattazione o di servizio, ma anche appunti o altro contenuto diverso da quello rilevante.

Tanto che con tecniche di steganografia[11] si possono inserire byte comportanti altro, e perché no anche una dichiarazione negoziale, in un file che un programma leggerebbe come immagine od altro.

---

[8] E non a caso Ulpiano ha definito la giurisprudenza, oltre che scienza del giusto e dell'ingiusto, come conoscenza delle realtà umane e divine.

[9] Così ad esempio caratteri di testo possono essere codificati in uno o più byte a secondo del numero dei caratteri, immagini inserite in una matrice di bit, suoni campionati, etc.

[10] La scelta di mostrare, convertendoli dal binario (base due e quindi due cifre) all'esadecimale (base 16 e quindi sedici cifre, utilizzandosi oltre i numeri dallo 0 al 9, per le restanti 6 le prime sei lettere dell'alfabeto, da A a F), i singoli byte in formato esadecimale è dovuta alla comodità di rappresentare un byte, costituito da 8 cifre binarie, in sole due cifre esadecimali comprese tra 00 e FF.

[11]La steganografia è la tecnica di nascondere informazioni in altre informazioni per renderne più difficile l'individuazione.

Addirittura è stato possibile elaborare in passato, a scopo dimostrativo, file che aperti con un programma di grafica mostravano una dichiarazione contrattuale per un certo prezzo ed aperti con un programma per pagine web mostravano un prezzo assai differente.

Quindi nel valutare un documento informatico come definito dalla lettera p) del primo comma dell'art. 1 del d.lgs. 7 marzo 2005 n. 82 e cioè come "il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti", occorre prima sapere e concordare come tale rappresentazione sia codificata, non essendo ciò immediatamente intellegibile. Se può soccorrere il criterio dell'*id quod plerumque accidit* (quello che comunemente accade) e quindi una presunzione, non è detto che ciò accada nel 100% dei casi.

Tale incertezza insita nel documento informatico è comunque superabile dall'imposizione normativa o pattizia di formati standardizzati e quindi leggibili da programmi specifici.

Il formato ed il documento informatico però non hanno nulla a che vedere con come il file sia memorizzato in un supporto, con il suo nome e con la sua estensione.

L'insieme di byte che identificano il documento informatico non contengono infatti tali informazioni. Queste sono infatti contenute nel così detto *file system* che è una struttura dati deputata alla gestione e all'archiviazione dei file in un supporto di memorizzazione, per capirsi, come una sorta di schedario di una biblioteca. Se per mera comodità e facilità di uso, oltre alle informazioni su dove trovare il file (che può anche essere disperso in vari blocchi nel supporto) c'è anche il nome del file, questo nome con il documento informatico propriamente inteso non ha nulla a che fare. Tanto che se si cambia il nome di un file munito di firma digitale, quest'ultima rimane valida e rimane valida semplicemente perché tale nome non fa parte di quel documento informatico e quindi, modificando il nome, non si è cambiato neanche un bit del documento.

Se poi il *file system* di riferimento, sempre per comodità, prevede l'uso di estensioni, cioè di parti alla fine del nome, normalmente precedute da un punto, anche tale informazione è estranea al documento informatico a cui si è voluto attribuire quel nome con quella data estensione. L'estensione ha normalmente lo scopo di indicare al sistema operativo con quale programma tentare di aprire automaticamente il documento stesso. Tentare perché non è detto che il documento sia in quel formato e l'estensione potrebbe mancare totalmente senza con ciò pregiudicare la possibilità di utilizzare il programma *ad hoc* per aprire quel file.

Quindi il fatto che il nome di un documento informatico abbia una certa estensione non implica che quel documento possa essere aperto con il programma associato a quell'estensione, né che il documento abbia il formato collegato a quell'estensione. Così come la mancanza di una estensione o la presenza di altra estensione in un documento informatico firmato digitalmente non inficia la firma stessa. In altre parole non si può affermare che una firma digitale esiste perché il relativo file ha una data estensione e quindi si capisce il *bias* in cui è incorsa la Cassazione nelle motivazioni riportate all'inizio del presente articolo.

Così il formato pdf (*portable document format*), vale a dire quel formato di file standardizzato introdotto da Adobe e che facilita lo scambio di documenti digitali mantenendo anche lo stesso aspetto grafico, incapsulando in sé anche documenti di varia natura (testo, immagini, etc.), è un qualcosa di diverso dall'estensione .pdf che può essere presente nel *file system* nel nome di un file: un file con estensione .pdf non necessariamente è nel formato pdf, così come un file con estensione diversa o senza estensione può invece esserlo ed essere quindi aperto con un programma in grado di trattare quel formato.

Attualmente normativamente le firme digitali possono avere tre diversi formati cd. "busta", nel senso che in un stesso file/documento coesistono il documento firmato, il documento

costituente la firma ed il certificato digitale che in astratto, come sarà esposto, potrebbero anche essere e/o viaggiare separati.

Si tratta del formato CAdES (p7m), utilizzabile per qualsiasi documento quale che sia il suo formato, il formato PAdES (pdf) integrato nello standard pdf e quindi utilizzabile solo per firmare file in quel formato ed il formato XAdES (xml) integrato nello standard xml e quindi utilizzabile solo per file in quel formato[12].

Ma, e per l'estensione dovrebbe essere ormai chiaro il perché, neanche il formato corretto garantisce che ci sia una firma digitale valida.

La crittografia a doppia chiave[13], pubblica cioè conoscibile potenzialmente da tutti e privata da tenere segreta, consente appunto l'apposizione di una firma elettronica su un documento informatico attraverso prima l'estrazione della sua "impronta digitale informatica" per mezzo di una funzione di hash[14] che

[12] Ad esempio attualmente l'Agenzia delle Entrate firma in XAdES le ricevute di trasmissione delle fatture elettroniche al sistema di interscambio. Quella firma elettronica però non è una firma digitale bensì una firma elettronica avanzata in quanto il certificato usato non è qualificato. Pur cambiando in questo caso poco ai fini del valore pratico della firma è evidente che il sistema normativo attuale delle firme elettroniche presenta delle discrasie: ad esempio non è una firma elettronica qualificata, sempre per mancanza dell'attributo di qualificato del certificato, ma una firma elettronica avanzata, anche quella ottenuta attraverso l'uso del certificato di firma rilasciato dal Ministero dell'Interno e presente nelle carte di identità elettroniche.

[13] Dove la chiave pubblica può decriptare quanto criptato dalla chiave privata e viceversa. Attualmente è basata sulla matematica della fattorizzazione dei numeri primi che per lo standard attuale, non conoscendosi algoritmi veloci per la fattorizzazione di numeri interi molto lunghi, rende sostanzialmente impossibile anche per un potente calcolatore ricavare in tempi umani la chiave privata da quella pubblica. La situazione cambierebbe con l'avvento di computer quantistici in grado di violare la crittografia attuale con una vera e propria ecatombe informatica, economica e giuridica a meno che prima non vengano elaborati algoritmi cd. post quantistici basati su problemi matematici la cui soluzione sfugga anche a tale capacità di elaborazione. Al riguardo cfr. HOUSTON EDWARDS, *Segreti a prova di quanti*, in *Le Scienze*, aprile 2024, 58.

[14] Le funzioni di hash sono funzioni matematiche con esecuzione veloce che a partire da una sequenza di bit di lunghezza n restituiscono una stringa di lunghezza di bit predeterminata e devono godere di due proprietà fondamentali: che sia "complicato" trovare due oggetti che abbiano lo stesso hash e che sia "complicato" a partire da un hash trovare un documento che produca, attraverso la funzione, lo

ritorna una stringa di lunghezza fissa qualunque sia la lunghezza del documento e poi attraverso la cifratura dell'hash con la chiave segreta del firmatario. La verifica viene effettuata attraverso la decifratura dell'hash criptato con la chiave pubblica del firmatario, l'estrazione dell'hash dal documento ed il confronto dell'hash decriptato con quello estratto. Se sono uguali la firma è verificata.

Il tutto è facilitato dall'uso di certificati digitali, cioè da file che contengono vari dati tra cui la chiave pubblica del firmatario che possono essere generati direttamente da quest'ultimo, da terzi più o meno affidabili o, come nel caso delle firme digitali, da certificatori qualificati con un sistema pubblicistico di accreditamento che quindi garantiscono legalmente la corrispondenza del certificato ad un dato titolare, firmandolo a loro volta, e forniscono i relativi dispositivi sicuri di firma con all'interno la chiave segreta.

I formati di cui sopra hanno la funzione di incapsulare per praticità la firma, che essendo costituita dall'hash del documento criptato con la chiave segreta potrebbe tranquillamente essere in un file a sé stante, ed il certificato nel documento firmato ma ovviamente, anche nel caso di firma digitale, non sono garanzia del fatto che ci sia una firma valida.

Ricordando che il regolamento europeo eIDAS prevede in generale la neutralità tecnologica[15] , esso norma per le firme elettroniche qualificate all'art. 28 i requisiti dei certificati qualificati e agli artt. 29 e 30 i requisiti per i dispositivi di firma e relativa certificazione.

L'art. 32 stabilisce i requisiti per la convalida delle firme elettroniche qualificate e quindi anche delle firme digitali per cui "il processo di convalida di una firma elettronica qualificata

stesso hash. Si usano per le firme in modo da evitare la crittografia dell'intero documento con le relative complicazioni, lunghezza e tempi compresi.

[15] XXVII considerando: "È opportuno che il presente regolamento sia neutrale sotto il profilo tecnologico. È auspicabile che gli effetti giuridici prodotti dal presente regolamento siano ottenibili mediante qualsiasi modalità tecnica, purché siano soddisfatti i requisiti da esso previsti".

conferma la validità di una firma elettronica qualificata purché: a) il certificato associato alla firma fosse, al momento della firma, un certificato qualificato di firma elettronica conforme all'allegato I; b) il certificato qualificato sia stato rilasciato da un prestatore di servizi fiduciari qualificato e fosse valido al momento della firma; c) i dati di convalida della firma corrispondano ai dati trasmessi alla parte facente affidamento sulla certificazione; d) l'insieme unico di dati che rappresenta il firmatario nel certificato sia correttamente trasmesso alla parte facente affidamento sulla certificazione; e) l'impiego di un eventuale pseudonimo sia chiaramente indicato alla parte facente affidamento sulla certificazione, se uno pseudonimo era utilizzato al momento della firma; f) la firma elettronica sia stata creata da un dispositivo per la creazione di una firma elettronica qualificata; g) l'integrità dei dati firmati non sia stata compromessa; h) i requisiti di cui all'articolo 26[16] fossero soddisfatti al momento della firma".

Se quindi i software forniti dai certificatori autorizzati sono affidabili per le verifiche e lo stesso regolamento eIDAS prevede la possibilità all'art. 33 di un servizio di convalida qualificato delle firme elettroniche qualificate, è evidente che non solo non ci si può fermare al formato dei documenti informatici da verificare, che è solo un punto di partenza quando normativamente prescritto, ma è sempre necessario provvedere alla verifica.

Verifica che può essere antecedente all'inserimento di un documento in un fascicolo giudiziario informatico o successiva, ma che deve essere necessariamente controllata o rieffettuata quando ci sia un dubbio o una contestazione in merito.

In tal caso occorre essere sicuri della bontà del software (che può essere anche di terzi rispetto ai certificatori) utilizzato ed interpretarne correttamente i risultati. Ad esempio per la firma digitale è previsto che dal giugno 2011 l'unico algoritmo di hash

[16] Che sono quelli della firma elettronica avanzata, requisiti che anche la firma elettronica qualificata deve avere oltre agli ulteriori due che ad essa sono peculiari.

utilizzabile sia lo SHA256[17] , per cui eventuali errori segnalati dal software dovuti a questo sono irrilevanti se il documento è stato sottoscritto prima di tale data. Così se il certificato di firma è scaduto al momento della verifica, occorre accertare se il documento è stato sottoscritto quando era ancora valido. Inoltre una verifica completa di una firma digitale può essere effettuata solo avendo l'accesso alla banca dati dei certificati revocati del fornitore qualificato e controllando che alla data della firma il certificato utilizzato non sia stato revocato. Se quindi il software restituisce un errore per non aver potuto compiere tale verifica o non la compie, la sicurezza della verifica ci sarà solo quando anche questo ulteriore passo sarà effettuato. Nel formato PAdES poi il software, specie se si usa quello di Adobe, potrebbe segnalare un errore come "almeno una delle firme non è valida" o "il documento dopo la firma è stato modificato o si è danneggiato", errore dovuto ad una modifica, ad esempio per l'apposizione di un numero di protocollo od altro, al file già sottoscritto ma che non inficia la firma digitale relativa al documento non modificato posto che detto formato comunque conserva anche la versione del documento firmata precedentemente alla modifica che quindi può essere esaminata.

Conclusivamente il processo di verifica di una firma digitale e dei suoi effetti giuridici non è affatto banale e soprattutto non può essere ristretto alla constatazione dell'esistenza di un dato formato del documento e/o di una certa estensione nel nome.

[17] Mentre prima era utilizzato lo SHA1, per la cronaca ancora utilizzato oggi per le firme elettroniche dei messaggi di posta elettronica certificata da parte dei relativi fornitori.