LA DATA CERTA E L'EQUIVOCO SUGLI ALLEGATI ALLA POSTA ELETTRONICA CERTIFICATA

MASSIMO EROLI

L'art. 2704 c.c. prevede che "*la data della scrittura privata della quale non è autenticata la sottoscrizione non è certa e computabile riguardo ai terzi, se non dal giorno in cui la scrittura è stata registrata o dal giorno della morte o della sopravvenuta impossibilità fisica di colui o di uno di coloro che l'hanno sottoscritta o dal giorno in cui il contenuto della scrittura è riprodotto in atti pubblici o, infine, dal giorno in cui si verifica un altro fatto che stabilisca in modo egualmente certo l'anteriorità della formazione del documento*"

Perché quindi una scrittura privata, ma anche un'altra prova documentale per cui occorra dimostrare l'anteriorità della sua formazione rispetto ad una certa data, abbia tale caratteristica è sufficiente un collegamento, anche a mezzo di presunzioni semplici, con un fatto temporalmente certo che possa fare inferire che il documento di cui ci si sta occupando sia venuto ad esistenza prima di tale fatto.

Si ricorda che ai sensi dell'art. 2729 c.c., che stabilisce che le presunzioni debbano essere gravi, precise e concordanti, non occorre che tra il fatto noto e quello ignoto sussista un legame di assoluta ed esclusiva necessità causale, ma è sufficiente che il fatto ignoto derivi da quello noto come conseguenza ragionevolmente possibile e verosimile secondo criteri di normalità (da ultimo Cass. 18 gennaio 2021, n. 703; Cass. 28 settembre 2020, n. 20342).

Così uno dei modi più usati per raggiungere tale risultato era in passato l'apposizione sul foglio contenente lo scritto del timbro postale datario (cfr. Cass. 6 luglio 2020 n. 13920), tra l'altro ancora oggi utilizzato per gli atti notificati direttamente dagli avvocati a mezzo posta ex l. 53/94.

A seguito della dismissione da parte delle poste di detto servizio generalizzato e grazie all'introduzione dei servizi digitali, si sono utilizzate marche temporali (ora ex artt. 41 e 42 reg. UE 910/2014) o marche postali elettroniche (ex d.p.c.m. 14 dicembre 2010).

Marche temporali digitali, quando si tratta di documenti analogici, necessariamente apposte su copie informatiche per immagine degli stessi.

Una copia informatica per immagine munita così di data certa fa infatti presumere che il corrispondente documento analogico sia anch'esso munito di data certa (cfr. da ultimo Trib. Catania (ord) 11 gennaio 2018).

Interessante anche rilevare come il citato Regolamento Ue eIDAS contenga una nozione ampia di validazione temporale elettronica.

Al primo comma dell'art. 41 infatti prevede che "*alla validazione temporale 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 della validazione temporale elettronica qualificata*", requisiti questi ultimi che ai sensi dell'art. 42 sono: a) collegamento della data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati; b) utilizzo di una fonte accurata di misurazione del tempo collegata al tempo universale coordinato; c) apposizione mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.

Va sottolineato che la validazione temporale e quindi la data certa di una prova documentale prescinde dalla natura di detto documento, natura che costituisce un problema distinto e a sé

stante e che unita alla validazione temporale può comportare o meno la sua validità, sostanziale o come elemento probatorio.

Così ad esempio la validazione temporale di una copia informatica per immagine di una scrittura privata comporta che l'originale analogico di detta scrittura privata, pur non essendo direttamente munito di validazione temporale, abbia data certa in quanto costituisce una presunzione grave, precisa e concordante che quel documento analogico non possa essere stato realizzato dopo la sua copia informatica per immagine.

Inoltre non è necessario per tale specifico fine che detta copia informatica per immagine sia sottoscritta elettronicamente, essendo appunto sufficiente che sia una semplice copia mentre i requisiti di forma propri della scrittura privata vanno verificati sull'originale.

Ovviamente, in caso di contestazione della conformità, è necessaria la produzione anche dell'originale analogico secondo le regole generali.

Quindi un conto è la validazione temporale di un documento, un altro la sua natura e le sue caratteristiche anche formali.

Se si tratta di scrittura privata è evidente che per essere tale l'originale di essa deve essere sottoscritto. Se la scrittura privata è informatica la sottoscrizione deve risultare dall'originale o, il che è lo stesso, da un suo duplicato informatico.

Ma quando la scrittura privata è informatica la sottoscrizione può risultare, qualora non sia prevista la forma scritta *ad substantiam*, da una firma elettronica semplice secondo il libero apprezzamento del giudice in relazione alla sua caratteristica oggettiva di qualità, sicurezza, integrità e immodificabilità e qualora sia prevista la forma scritta *ad substantiam*, da minimo una firma elettronica avanzata (cioè che dia la garanzia univoca di connessione al firmatario, sia creata con mezzi di cui il firmatario può conservare un controllo esclusivo con un elevato livello di sicurezza e sia collegata ai dati a cui la firma si riferisce che consente di rilevare se i dati siano stati modificati successivamente alla firma) per gli atti di cui al n. 13 dell'art. 1350 c.c. e per i restanti atti di cui all'art. 1350 c.c. da una firma

elettronica qualificata (che ha in più di quella avanzata l'uso di un dispositivo sicuro di firma e di un certificato elettronico qualificato).

L'introduzione in Italia della posta elettronica certificata, seguita dall'introduzione in ambito europeo dei servizi elettronici di recapito certificato (artt. 43 e 44 eIDAS), ha costituito indirettamente anche un modo facile ed economico per attribuire la data certa a un documento.

Infatti il messaggio di posta elettronica certificata che arriva al destinatario e la ricevuta di consegna per il mittente che contiene direttamente o indirettamente, a secondo del tipo, anche il messaggio originale sono muniti di firma elettronica avanzata del gestore di posta elettronica che contiene anche la data e l'ora, dati che provenendo da un soggetto terzo affidabile, sono considerabili certi.

Per i servizi elettronici di recapito certificato previsti da eIDAS inoltre l'art. 43 prevede che "*ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato*" e che "*i dati inviati e ricevuti mediante servizio elettronico di recapito certificato qualificato godono della presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate dal servizio elettronico di recapito certificato qualificato*".

Al momento non tutti i servizi di posta elettronica certificata italiani soddisfano (anche se possono farlo) tutti i requisiti eIDAS per i servizi elettronici di recapito certificato che sono secondo l'art. 44: a) la fornitura da uno o più prestatori di servizi fiduciari qualificati; b) la garanzia con un elevato livello di sicurezza dell'identificazione del mittente; c) la garanzia dell'identificazione del destinatario prima della trasmissione dei

dati; d) la garanzia dell'invio e la ricezione dei dati da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati; e) l'indicazione chiara di qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli al mittente e al destinatario dei dati stessi; f) l'indicazione della data e dell'ora di invio e di ricezione e qualsiasi modifica dei dati da una validazione temporale elettronica qualificata.

Ciò però non è rilevante ai fini della nostra indagine, considerato che i requisiti eventualmente mancanti non attengono alla certezza della data del messaggio o della ricevuta di consegna della posta elettronica certificata.

A questo punto va chiarito un primo equivoco, se non addirittura un bias, che deriva dalla stessa natura dei documenti informatici.

Si tende infatti a confondere la sostanza giuridica di un insieme di bit con il file in cui sono contenuti, dimenticando che ciò che è all'interno del file (esso stesso frutto dell'accorpamento codificato di una serie di bit non necessariamente contigui presenti nel supporto dove è memorizzato) è solo una pluralità di bit che codifica delle informazioni che non solo devono essere decodificate da un programma ma il loro contenuto visibile può essere diverso a seconda del programma che si utilizza.

Quindi, anche per i formati di file più comunemente usati, all'interno del file ci potrebbero essere informazioni che potrebbero essere giuridicamente rilevanti in riferimento alla volontà dell'autore (nulla ad esempio vieterebbe di inserire una proposta contrattuale in un file immagine alterando singoli byte con tecniche di steganografia digitale).

Ciò è tanto più vero per i cd. formati di incapsulamento dove all'interno dei singoli file ci sono pezzi di informazione che potrebbero essere anche a sé stanti, collegati tra loro od anche non collegati.

Per rendersene conto basta aprire un qualsiasi file con un editor esadecimale come XVI32 che mostra byte per byte visualizzati come due cifre esadecimali il contenuto del file e, in una finestra separata, l'eventuale corrispondenza in codice ASCII evidenziando così anche eventuali parti di testo puro codificate in ASCII.

La posta elettronica certificata si basa sugli stessi standard della posta elettronica normale con la particolarità più rilevante che il servizio è fornito da prestatori qualificati che firmano elettronicamente il messaggio di posta che arriva al destinatario e le ricevute di accettazione e di consegna che arrivano al mittente attestandone anche la data e l'ora.

Questi sono file che possono essere memorizzati in formati come .eml (il più diffuso) o .msg (proprietario Microsoft) ed al loro interno contengono informazioni di servizio, tra cui i cd. headers, la codifica del messaggio principale in formato testo, html o quant'altro, e qualsiasi altro pezzo di informazione come i cd. allegati, posto che lo standard della posta elettronica consente di trasmettere all'interno del messaggio di posta qualsiasi file.

Ed al loro interno c'è anche la firma elettronica del gestore della posta elettronica del mittente per il messaggio di pec che arriva al destinatario e per la ricevuta di accettazione che arriva al mittente e del gestore della posta elettronica del destinatario per la ricevuta di consegna che arriva al mittente.

Si tratta di firme elettroniche avanzate e non di firme elettroniche qualificate in quanto mancano di alcuni degli elementi previste per queste ultime (ad esempio l'algoritimo di hash è ancora SHA1 e non SHA256) ma non per questo meno affidabili considerata la normativa che regola il servizio.

Tale firma elettronica altro non è che la codifica con la chiave segreta del gestore dell'impronta digitale del file (il cd. hash) per cui decodificandola con la chiave pubblica e confrontandola con quella ottenuta autonomamente utilizzando l'algoritmo di hash una eventuale difformità indica l'alterazione anche di un solo bit

del file (firma elettronica esclusa ovviamente che pur essendo nel file non fa parte del contenuto firmato).

Non sono ovviamente firmati neanche gli attributi del file, come nome ed estensione, in quanto non fanno parte del file stesso.

Tutto il resto è però firmato, compresi gli eventuali allegati, e tale firma certifica sia che non ci sono state alterazioni rispetto a quanto trasmesso, sia la data ed ora in cui la trasmissione e la generazione della ricevuta è avvenuta.

Se non si è convinti di ciò, ma è negli standard del servizio, basta aprire un file .eml o msg. di pec con allegati con XVI32, modificare anche un solo byte relativo ad uno degli allegati e controllare la firma del file risultante che non sarà più valida segnalando quindi la modifica.

Da ciò ne consegue che tutto il contenuto del file oggetto di sottoscrizione da parte dei gestori ha data certa nel senso che non può essere successivo a tale firma.

Senza quindi alcuna distinzione tra testo principale del messaggio ed eventuali allegati.

Chiarito questo è evidente che nel messaggio di posta elettronica certificata e nella ricevuta di consegna ci possono essere più documenti informatici il cui significato giuridico ed i collegamenti tra di loro vanno analizzati ed interpretati.

Anche l'imputazione giuridica di essi a determinati soggetti è tutta da verificare ma questo è appunto vero per tutti i documenti con un significato giuridico a sé stante contenuti nel messaggio, sia che siano nel testo principale sia che siano allegati.

Semplicemente l'allegato è qualcosa che solo da un punto di vista tecnico non può essere inserito nel testo principale ma in altra parte del file sottoscritto dai gestori.

La prima operazione da fare, si ripete indistinta tra testo principale ed allegati, è quindi l'esame del contenuto di questi documenti.

Ad esempio se io, non contraente, mi auto spedisco una pec con allegata la copia informatica per immagine di un contratto

analogico concluso tra altri soggetti che prima non aveva data certa, è evidente che quel contratto avrà per effetto di questa spedizione data certa ma è altrettanto evidente che nessun effetto giuridico sarà a me imputabile e le sottoscrizioni di quel contratto saranno quelle dell'originale analogico.

Se quindi nel testo principale o negli allegati ci sono dichiarazioni negoziali occorrerà vedere se e a chi possono essere imputabili.

Se poi tali dichiarazioni richiedono forma scritta e sono contenute esclusivamente in documenti informatici occorrerà anche verificare se e di chi contengono firme elettroniche e, se occorre una precisa tipologia di firma elettronica, ad esempio avanzata o qualificata, se tale requisito sia rispettato.

Se è certo chi sia l'intestatario della pec e sussistano sufficienti garanzie di sicurezza sull'uso di quella pec da parte di quel soggetto determinato e nel testo e negli allegati ci sono dichiarazioni negoziali di quest'ultimo, queste saranno anche sottoscritte dal mittente con firma elettronica avanzata, ricorrendo in tal caso tutti gli elementi di questa o, dove ne manchi alcuno, semplice con conseguente valutazione caso per caso degli elementi che possono o meno attribuire la forma scritta.

Altrimenti sarà necessario firmare elettronicamente con la tipologia di firma appropriata le parti dove ci sono tali dichiarazioni, sia che si tratti di allegati, sia che si tratti del testo principale (per ulteriore informazione è infatti possibile firmare elettronicamente anche il testo di una pec ed anche una mail semplice).

A questo punto è evidente quali siano gli equivoci in cui si può incorrere a causa della recente Cass. 15 aprile 2024 n. 10091.

In quel caso il giudice di merito aveva ritenuto non opponibile ad una procedura fallimentare un contratto di affitto di azienda analogico per mancanza di data certa.

L'opponente, società a responsabilità limitata, inferiva la presenza della data certa da una pec di tre anni dopo l'asserita

conclusione di tale contratto con cui essa aveva chiesto il pagamento dei canoni insoluti imputandoli a tale contratto di cui, sembra in una nota allegata a tale pec, aveva descritto i tratti essenziali.

Il Tribunale aveva ritenuto che se tale nota fosse stata dotata di data certa avrebbe esteso la certezza della data alla scrittura privata ed alle previsioni essenziali in essa contenuta.

Tuttavia ha stabilito che nel caso di specie c'era solo la prova dell'invio della pec ma non anche che il documento allegato alla pec fosse la nota prodotta.

Ciò in quanto il documento non era stato prodotto in formato elettronico e quindi non era possibile verificare se allegata alla pec vi fosse effettivamente la comunicazione prodotta.

Il che è ineccepibile in quanto i documenti informatici vanno prodotti (anche prima dell'obbligatorietà del pct) nel relativo formato informatico. Nella specie avrebbe dovuto essere prodotta la ricevuta di consegna della pec in formato .eml o .msg. oppure qualora la tipologia di ricevuta non fosse quella completa, cioè con allegato il messaggio inviato, anche il messaggio inviato sempre in formato .eml o .msg per consentirne la comparazione con l'hash riportato nella ricevuta.

La Cassazione ritiene però di dover correggere tale motivazione in diritto.

Richiama innanzitutto Cass. 20 novembre 2023 n. 32165 che avrebbe negato che il documento allegato ad una pec sia attratto dal regime di quest'ultima.

In realtà in quel caso si trattava del disconoscimento di un atto di cessione di credito allegato ad una pec senza che fosse seguita istanza di verificazione, sostenendo invece il mittente che quel documento era allegato ad una pec e sarebbe stato attratto al regime di quest'ultima, cioè opponibile a terzi e vincibile solo con consulenza tecnica volta a dimostrare che l'atto, dal punto di vista informatico, non proviene da chi ne certifica l'invio.

Affermazione palesemente non vera.

Il giudice di legittimità infatti puntualizza che una pec significa attestare che essa proviene dal mittente, che contiene quanto allegato (sic) e che è stata inviata a quell'ora; ma non significa attestare altresì la veridicità di ciò che è allegato. La posta elettronica certificata dimostra l'invio e la ricezione del messaggio, ma non garantisce il contenuto del documento allegato.

Ma, attenzione, non nel senso che il documento allegato non sia quello ma nel senso che quando non è un duplicato informatico ma una copia, il documento originale, ovviamente non allegato alla pec, potrebbe anche essere diverso.

Specifica infatti la Cassazione: "*si supponga il caso in cui con posta certificata si invia un documento dal falso contenuto, o proveniente da un terzo: si dovrebbe dire che, avendo il mittente certificato la posta (ossia attestato che proviene da lui e che è stata spedita a quell'ora) ha altresì attestato che il documento allegato è vero o che è riferibile ad un terzo*."

Equivocando tale pronuncia, Cass. 15 aprile 2024 n. 10091 arriva ad affermare che "*la Pec è in grado di attestare in maniera certa l'avvenuta trasmissione e ricezione del messaggio, le modalità di spedizione (data, ora e formato) ed anche il suo contenuto, ma limitatamente alla Pec stessa, non al file allegato ad essa. Pertanto, se alla Pec è stato allegato un file con un determinato nome, estensione, formato e dimensioni la ricevuta lo attesterà, ma non farà prova del contenuto di quel file*".

In realtà, per quanto sopra esposto, la pec è perfettamente idonea a provare il contenuto degli allegati, *rectius* che contiene quanto allegato, non è invece idonea a provarne di per sé la veridicità fattuale.

Si auspica quindi che lettori frettolosi non amplifichino tale equivoco, come accaduto in passato per altre pronunce della Cassazione in materia di informatica giuridica.

Per la cronaca la Cassazione ha anche censurato l'affermazione del Tribunale secondo cui la data certa di un documento che richiama, al suo interno, il contenuto di un

contratto nei suoi tratti essenziali estenderebbe la certezza della data anche alla scrittura privata ed alle previsioni essenziali in essa contenute, ma questa ci sembra più questione di merito relativa al collegamento di quell'atto avente data certa con quello a cui sarebbe da attribuire tale data.