IP, IT e Data protection

I documenti informatici: nuovi linguaggi e processo civile

La disciplina del CAD e del Codice civile, l'efficacia probatoria e le modalità di disconoscimento

Ricorre l'esigenza di un'ulteriore rilettura della disciplina concernente i **documenti informatici** in considerazione dell'esponenziale incrementarsi dell'uso, nel nostro quotidiano, dei formati **video e audio** la cui gestione, nell'ambito del processo necessariamente, si inserisce nel solco della tradizionale bipartizione tra trasmissione e consultazione [1], a seconda che trattasi di atti o di documenti allegati.

È imminente la possibilità di allegare nel processo telematico documenti informatici anche nei formati Video: MPEG2 e MPEG4 (.mp4, .m4v, .mov, .mpg, .mpeg), AVI (.avi) e Suono: MP3 (.mp3), FLAC (.flac), audio RAW (.raw), Waveform Audio File Format (.wav), AIFF (.aiff, .aif).

Su tali presupposti è possibile svolgere alcune riflessioni ricorrendo al generale concetto di documento: qualunque oggetto materiale e immateriale idoneo a rappresentare o dare conoscenza di un fatto; con l'ulteriore distinzione che, nel processo, la **rappresentazione** può essere immediata o realizzarsi anche in termini mediati, quale prova del fatto. Ad esempio un documento può rappresentare la stipulazione di un contratto ed è la prova immediata del fatto storico perché contiene lo scambio di consensi in ordine ad un certo oggetto. Al contrario la quietanza non è la prova immediata dell'avvenuto pagamento ma attesta semplicemente che una parte ha dichiarato di aver ricevuto una certa somma da un terzo, definibile come una prova di un'altra prova che ha per oggetto il fatto avvenuto, cioè il pagamento[2]. Un **video** può rappresentare un incidente stradale e nel processo può essere introdotto anche un filmato di un soggetto che si limita a raccontare come è accaduto il sinistro. Con l'ulteriore conseguenza che, nella rappresentazione non immediata, diviene indispensabile la verifica sul soggetto che ha reso la dichiarazione, del destinatario così come del contesto in cui ciò è avvenut**o.**

Sommario

1. Fonti

La fonte primaria di riferimento per il **documento informatico** è il Codice dell'Amministrazione Digitale – CAD, **D.lgs. 7 marzo 2005, n. 82** e successive modificazioni. Tra le definizioni di cui all'art. 1, la lett.p) è dedicata al **documento informatico** quale **rappresentazione informatica** di atti, fatti o dati giuridicamente rilevanti[3].

L'intento principale del CAD è di regolamentare i diritti di cittadinanza digitale e di riconoscere le tecnologie dell'informazione e della comunicazione come prioritario strumento per la promozione nei rapporti tra cittadini, imprese e pubbliche Amministrazioni in attuazione degli indirizzi per la digitalizzazione [4]. La rilevanza giuridica da veicolarsi nel processo ed in particolare in quello civile necessita di regole a mezzo di legislazione primaria e secondaria che in parte è confluita nel CAD, in attuazione di un'indiscussa esigenza di codificazione.

Nel CAD, la Sezione I del capo II, articoli da 20 a 23 quater è dedicata al **documento informatico** e, dalla sua impostazione, è evidente l'intento di non discostarsi dal collaudato sistema del codice civile e di quello di rito, come comprovato dalla scelta di disciplinare la validità e **l'efficacia probatoria** dei **documenti informatici**, nel medesimo sistema codicistico di cui agli **artt. 2702 e ss c.c.**[5].

2. Un possibile contemperamento

Ricorre, a mio avviso, l'esigenza di contemperare: a) l'assoggettamento del **documento informatico** alla sua libera valutazione in giudizio in relazione alle caratteristiche di sicurezza, integrità e immodificabilità al fine di stabilirne l'idoneità a soddisfare il requisito della forma scritta e il suo **valore probatorio** come stabilito dalla seconda parte dell'art.20.1 bis CAD, con b) il successivo art.23 quater per il quale le **riproduzioni informatiche** sono regolate dall'art. 2712 c.c. (espressamente inserite dopo le parole riproduzioni fotografiche) caratterizzato dal sistema del possibile **disconoscimento** e, in mancanza, dell'efficacia di piena prova.

Al contempo va evidenziato che gli artt.20 e ss del CAD si riferiscono al **documento informatico** nella sua valenza di *genus* rispetto alla *species* della scrittura privata, con la possibilità di distinguerne le relative discipline.

Vi è, quindi, il **documento informatico** che non rappresenta una **scrittura privata informatica**, pur risultandone essenziale la sua idoneità a soddisfare il requisito della forma scritta a rappresentare o a dare conoscenza diretta o indiretta di un fatto (rispetto alla successivamente trattazione del documento che rappresenta una scrittura privata digitale).

3. Prima scheda sinottica

Documento informatico	Documento informatico disconosciuto	Modalità del disconoscimento
Libera valutazione in giudizio in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. Al contempo ricorre la necessità anche di valutare gli effetti del non disconoscimento ai sensi dell'art.115 c.p.c.	La qualità di prova è degradata a presunzione semplice. Il documento può, in ogni caso, essere posto a base della decisione ricorrendo il giudice a una necessaria e concreta verifica con altri mezzi istruttori e in specie consulenze.	Tempestivo, chiaro, circostanziato ed esplicito. Con onore di allegazione di elementi attestanti la non corrispondenza tra realtà fattuale e realtà riprodotta. Il CNF, sent.234/2020, ha ritenuto di non poter escludere l'utilizzabilità delle registrazioni fonografiche a fronte di una non specifica contestazione dei fatti in modo chiaro, circostanziato ed esplicito, concernente la corrispondenza tra la realtà fattuale e quella riprodotta.

Ho inteso schematizzare le diverse possibili ipotesi in considerazione degli orientamenti della giurisprudenza di legittimità che ha espresso il principio secondo il quale, in tema di efficacia probatoria delle **riproduzioni informatiche** ex art. 2712 c.c., il **disconoscimento** idoneo a farne perdere la qualità di prova, degradandole a presunzioni semplici, deve essere non solo tempestivo, soggiacendo a precise preclusioni processuali, ma anche chiaro, circostanziato ed esplicito, dovendosi concretizzare nell'allegazione di elementi attestanti la non corrispondenza tra realtà fattuale e realtà riprodotta (Cass. Ord. 12794/2021 richiamata da C.App. Napoli 2023).

Nel termine **riproduzioni informatiche** sono ricomprese un elevato numero di strumenti di uso quotidiano: ad esempio un messaggio whatsapp, sia esso scritto o **audio**, una registrazione di un **video** o di un **audio**, un qualsivoglia file esistente su internet e così via. Se esse e con esse si rappresenta o sono fonte di conoscenza di un fatto del nostro agire, entrano nel processo così come la tradizionale stampa di una fotografia o di un documento cartaceo.

La prima parte dell'art.20.1–bis CAD precisa, inoltre, che il **documento informatico** soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'art. 2702 c.c. quando vi è apposta una firma digitale, altro tipo di **firma elettronica** qualificata o una **firma elettronica avanzata** o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'art.71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore.

Con detta norma, al requisito della forma scritta, si aggiunge la possibilità al **documento informatico** di acquisire l'efficacia prevista dall'art. 2702 c.c. e cioè quella della scrittura privata che, come detto, è da considerarsi una *species* del documento in quanto deve necessariamente esservi un autore e la conseguente imputabilità di quanto ivi rappresentato[6].

L'espresso richiamo all'**efficacia** di cui all'art.2702 c.c. sottopone il **documento informatico** sottoscritto (nelle dette modalità che garantiscono la sicurezza, l'integrità e immodificabilità in maniera manifesta ed inequivoca) alle regole delle scritture soggette a verifica di cui si schematizzano le maggiori caratteristiche.

4. Seconda scheda sinottica

Documento informatico sottoscritto a sensi dell'art.20.1 bis CAD col rinvio all'art.2702 c.c. e art.20.1 ter CAD	Sistema del riconoscimento tacito di cui all'art.215 c.p.c.	Disconoscimento ex artt.214 e 215 c.p.c. eventuale istanza di verificazione ex art.216 c.p.c.
L'efficacia è quella di piena prova fino a querela di falso della provenienza delle dichiarazioni. Con in aggiunta la riconducibilità della firma elettronica qualificata o digitale al titolare, salvo che questi dia la prova contraria.	Si conferma l'efficacia probatoria vincolante per il giudice in modo assoluto per il solo contenuto estrinseco e cioè riferito alla provenienza. Per il contenuto intrinseco permane il principio del libero convincimento. Ad eccezione, ad esempio, di una dichiarazione integrante confessione stragiudiziale sfavorevole	Tempestività, nella prima udienza o prima risposta successiva alla sua produzione. Nel ricorso in opposizione a d.i. – Cass.2.1.2024, n.55. Specificità e determinatezza – Cass. 2.1.2024, n.22.

L'art.21 co.2 bis CAD contiene anche una precisa disciplina delle **scritture private informatiche** con espresso rinvio all'art.1350 c.c.: "Salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350.1, numeri da 1 a 12, c.c., se fatte con **documento informatico**, sono sottoscritte, a pena di nullità, con **firma elettronica qualificata** o con **firma digitale**. Gli atti di cui all'art. 1350.1, numero 13, c.c. redatti su **documento informatico** o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale".

Per entrambe le ipotesi e cioè il mero **documento informatico** e quello rappresentante una scrittura privata sottoscritta con sicura imputabilità ad un autore è possibile evidenziare due aspetti comuni concernenti la rilevanza e il grado **efficacia probatoria**: a) il comportamento processuale delle parti tra acquiescenza e **disconoscimento**; b) le connesse e necessarie capacità tecnico valutative del giudicante e dei difensori.

Il **disconoscimento** del **documento informatico**, inteso nel suo ampio *genus*, si attua in modo chiaro, circostanziato ed esplicito denunciando necessariamente violazioni relative alla sua sicurezza, integrità e immodificabilità, con onore di allegazione di elementi attestanti la non corrispondenza della realtà digitalmente rappresentata e la verità (il termine sicurezza si riferisce a quella informatica e cioè alla protezione dei sistemi informatici, delle reti e dei dati da accessi non autorizzati, attacchi informatici, virus e altre minacce informatiche - a mezzo di firewall e altre misure di sicurezza - L'integrità del documento è la verifica su eventuali modifiche correlata al concetto di immodificabilità nel tempo. In ambiti informatici ricorrono i concetti di: Timestamp: L'apposizione di un timestamp al documento può essere utile per dimostrare che il documento esiste da un certo momento. I servizi di timestamping registrano la data e l'ora di creazione o modifica di un documento e forniscono un timbro temporale che può essere verificato successivamente. Autenticazione multi-fattore: Utilizzare un sistema di autenticazione multi-fattore per proteggere l'accesso ai documenti. Questo può includere l'uso di password sicure, autenticazione a due fattori - 2FA - o metodi biometrici. Catena di custodia: Mantenere una chiara catena di custodia per il documento, registrando ogni passo del suo percorso dalla creazione alla presentazione come prova. La documentazione accurata della catena di custodia aiuta a garantire che il documento non sia stato alterato o manipolato. Checksum e hash: Calcolare il checksum o l'hash del documento. Questa è una stringa di caratteri univoca che rappresenta il contenuto del documento. Anche una piccola modifica al documento cambierà completamente il suo checksum o hash. Può essere utilizzato per verificare l'integrità del documento. Archiviazione sicura: Conservare il documento in un ambiente sicuro e controllato per impedire l'accesso non autorizzato o manipolazioni. La protezione fisica è importante tanto quanto la sicurezza informatica. Registrazione degli accessi: Registra e monitora gli accessi al documento. La registrazione degli accessi può evidenziare eventuali tentativi di accesso non autorizzato. Standard di conservazione elettronica: Adottare gli standard di conservazione elettronica, se applicabili, che definiscono le pratiche per garantire l'integrità e l'autenticità dei documenti nel tempo).

5. Conclusioni ed esempi

Su tali considerazioni, è possibile domandarsi quali siano gli strumenti necessari per delegittimare il **documento informatico** o degradarne la sua **efficacia probatoria**.

In primo luogo, è indispensabile la completa consultabilità del documento in tutte le sue caratteristiche tecniche, tenuto soprattutto conto che i formati consentiti per le allegazioni sono molteplici: è diffusa la conoscenza dei formati maggiormente utilizzata quali pdf, jpeg, xml, mentre lo sono meno gli altri. Effettuata la consultazione, le verifica su eventuali violazioni informatiche non possono prescindere da approfondite conoscenze tecniche e gli avvocati necessariamente le devono o dovranno conoscere o averne contezza a mezzo di consulenti. Nella fase decisionale anche i magistrati a loro volta sono o saranno chiamati a conoscere tali peculiari aspetti. Ricorre la necessaria consapevolezza che le tecnologie per intervenire e modificare le fotografie, i video e gli audio sono sempre più sofisticate e diffuse soprattutto a mezzo dell'**intelligenza artificiale** mentre gli strumenti per le opportune verifiche sono meno reperibili e conosciuti e non sempre collaudati.

Ai fini di esempio, si ipotizza che l'oggetto della lite sia la validità di un contratto a distanza sottoscritto ai sensi dell'art.51.6 del D.Lgs. n. 206/2005 (Codice del Consumo) secondo il quale ricorre la possibilità che il contratto sia concluso per telefono con conseguenziale obbligo del professionista di confermare l'offerta al consumatore, il quale è vincolato solo dopo aver firmato l'offerta o dopo averla accettata per iscritto; in tali casi il **documento informatico** può essere sottoscritto con **firma elettronica**, con conferme da registrarsi su un supporto durevole.

Trattasi di un diffuso schema secondo il quale il consenso all'accordo non si raggiunge a seguito della mera telefonata perché ricorre la necessità che lo stesso venga reso espressamente, il più delle volte ciò avviene con l'invio di sms o di e-mail che, a sua volta, rimanda a una pagina web per la finalizzazione dell'accettazione del contratto a mezzo del sistema point e click.

Ipotizzando l'allegazione nel processo di un documento che rappresenta la ricostruzione informatica ed applicativa di quanto prescritto dal citato art.51, il consumatore a mezzo del suo difensore deve essere nelle condizioni, prima di poter di consultare il detto documento nelle sue complete caratteristiche tecniche per poi verificarne in che termini disconoscerne la validità denunziandone le violazioni ad es. concernenti la

sicurezza, l'integrità e l'immodificabilità, l'errore di imputazione, la non corrispondenza della realtà digitalmente rappresentata e quanto realmente accaduto e tutto ciò nei termini processuali al fine di non incorrere in decadenze. Al contempo, similari strumenti di controllo devono essere ad appannaggio del giudicante tenuto conto della costante e repentina evoluzione tecnologica e legislativa[7].

Le predette dinamiche processuali potrebbero avere ad oggetto anche **documenti informatici** con firma autentica[8] ed in tali casi, a mio avviso, similari conoscenze informatiche sono o dovranno essere possedute da parte del pubblico ufficiale in quanto è previsto che l'autenticazione della **firma elettronica** può avvenire anche mediante l'acquisizione digitale della sottoscrizione di qualsiasi altro tipo di firma elettronica avanzata previo accertamento della validità del certificato elettronico utilizzato e del fatto che il documento sottoscritto non sia in contrasto con l'ordinamento giuridico.

Nella consapevolezza che gli scenari che separano la realtà ed i mondi virtuali continueranno ad ampliarsi, l'auspicio è che nelle tutele dei diritti si riesca con tenacia e dedizione a smascherare ogni abuso informatico illecitamente architettato.

NOTE

1. Le Specifiche tecniche previste dall'articolo 34, co. 1 del DM 21 febbraio 2011 n. 44, concernente le regole tecniche per l'adozione delle tecnologie dell'informazione e della comunicazione nel processo civile e nel processo penale, delle tecnologie, disciplinano, all'art. 13, il Fascicolo informatico nei seguenti termini: 1. Il fascicolo informatico raccoglie i documenti (atti, allegati, ricevute di posta elettronica certificata) da chiunque formati, nonché le copie informatiche dei documenti; raccoglie altresì le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo. 2. Il sistema di gestione del fascicolo informatico, realizzato secondo quanto previsto all'articolo 41 del CAD, è la parte del sistema documentale del Ministero della giustizia che si occupa di archiviare e reperire tutti i documenti informatici, prodotti sia all'interno che all'esterno; fornisce pertanto ai sistemi fruitori (sistemi di gestione dei registri di cancelleria, gestore dei servizi telematici e strumenti a disposizione dei magistrati) tutti i metodi – esposti attraverso appositi web service – necessari per il recupero, l'archiviazione e la conservazione dei documenti informatici, secondo la normativa in vigore; l'accesso al sistema di gestione documentale avviene soltanto per il tramite dei sistemi fruitori, che gestiscono le logiche di profilazione e autorizzazione. 3. Le operazioni di accesso al fascicolo informatico sono registrate in un apposito file di log che contiene le seguenti informazioni: a) il codice fiscale del soggetto che ha effettuato l'accesso; b) il riferimento al documento prelevato o consultato (codice identificativo del documento nell'ambito del sistema documentale); c) la data e l'ora dell'accesso. 4. Il suddetto file di log è sottoposto a procedura di conservazione, sempre nell'ambito del sistema documentale, per cinque anni.

Pe poi dedicare il successivo CAPO III alla TRASMISSIONE distinguendo quella degli ATTI - art.14 (Formato dell'atto del procedimento in forma di documento informatico) 1. L'atto del procedimento civile o penale in forma di documento informatico, da depositare telematicamente nell'ufficio giudiziario, deve rispettare i seguenti requisiti: a) è in formato PDF o PDF/A; b) è privo di elementi attivi; c) è ottenuto dalla trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è pertanto ammessa la scansione di immagini; d) è sottoscritto con firma digitale o firma elettronica qualificata esterna secondo la struttura riportata ai commi seguenti; e) è privo di protezione di password; f) nel procedimento civile è corredato da un file in formato XML, che contiene le informazioni strutturate nonché tutte le informazioni della nota di iscrizione a ruolo, e che rispetta gli XSD riportati nell'Allegato 5; esso è denominato DatiAtto.xml ed è sottoscritto con firma digitale o firma elettronica qualificata. 2. La struttura del documento firmato è PAdES-BES (o PAdES Part 3) o CAdES-BES; il certificato di firma è inserito nella busta crittografica; è fatto divieto di inserire nella busta crittografica le informazioni di revoca

riguardanti il certificato del firmatario. La modalità di apposizione della firma digitale o della firma elettronica qualificata è del tipo “firme multiple indipendenti” o parallele, e prevede che uno o più soggetti firmino, ognuno con la propria chiave privata, lo stesso documento (o contenuto della busta). L’ordine di apposizione delle firme dei firmatari non è significativo e un’alterazione dell’ordinamento delle firme non pregiudica la validità della busta crittografica; nel caso del formato CAdES il file generato si presenta con un’unica estensione p7m. Il meccanismo qui descritto è valido sia per l’apposizione di una firma singola che per l’apposizione di firme multiple. 3. Le applicazioni di generazione della firma digitale o qualificata per la sottoscrizione dei documenti informatici devono utilizzare la funzione di hash di cui all'art 4, comma 2, del Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013. Al quale segue l’art.15 per la TRASMISSIONE dei DOCUMENTI INFORMATICI (Formato dei documenti informatici allegati).

2. Francesco P. Luiso in “Diritto processuale civile”, Milano 2019.

3. L’Italia nel 1997 si poneva all’avanguardia nel riconoscimento del **documento informatico** e nell’uso legale della firma digitale con l’art. 15 della L. 59/97 cd. Legge Bassanini – uno: “Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge”. L’impegno di innovazione legislativa negli anni successivi fu particolarmente rilevante con sinergie tra governo ed in particolare con i Notai, tra i quali il ricordo va ad una lezione particolarmente illuminante ed entusiastica del Notaio Mario Miccoli nelle nuove aule universitarie di Napoli Monte Santangelo, al quale si affiancarono non pochi altri notai napoletani. Lo scopo principale era l’interscambio con la P.A. ed in particolare con le Conservatorie, attribuendo validità giuridica ai documenti elettronici e alla sottoscrizione digitale.

4. **"Percorso per il decennio digitale"** è il programma strategico dell'UE per la trasformazione digitale. Fissa obiettivi e traguardi digitali specifici da raggiungere entro il 2030. Il programma mette in primo piano le competenze e l'istruzione digitali ed è articolato intorno a quattro settori: competenze, imprese, pubblica amministrazione e infrastrutture.

5. La consistenza risponde alla domanda: che cosa è la scrittura privata comprendendone i requisiti e gli elementi, mentre l’efficacia consiste nel complesso delle situazioni giuridiche che scaturiscono da essa; entrambe, la consistenza e l’efficacia, reciprocamente si equilibrano e si completano servendosi vicendevolmente –G. Laserra “La scrittura privata”, Napoli 1959.

6. La scrittura privata può, a seconda dei casi, contenere una mera dichiarazione di scienza o di natura negoziale e, quando proviene da un terzo, è declassata tra le cd. prove atipiche.

7. La Legge 214/2023 e cioè la legge annuale per il mercato e la concorrenza ha aggiunto al citato art.51 un ulteriore comma secondo il quale: “ In ogni caso, il consenso non è valido se il consumatore non ha preliminarmente confermato la ricezione del documento contenente tutte le condizioni contrattuali, trasmesse su supporto cartaceo o altro supporto durevole disponibile e accessibile”. Dopo l'articolo 65 è aggiunto il seguente: «Art. 65-bis (Contratti di servizi a tacito rinnovo). - 1. Nei contratti di servizi stipulati a tempo determinato con clausola di rinnovo automatico, il professionista, trenta giorni prima della scadenza del contratto, è tenuto ad avvisare il consumatore della data entro cui può inviare formale disdetta. La comunicazione di cui al primo periodo è inviata per iscritto, tramite sms o altra modalità telematica indicata dal consumatore, e la sua mancanza consente al consumatore, sino alla successiva scadenza del contratto, di recedere in qualsiasi momento senza spese».

8. Art.25 CAD “Firma autenticata” secondo il quale: Si ha per riconosciuta, ai sensi dell'articolo 2703 c.c., la firma elettronica o qualsiasi altro tipo di firma ((elettronica)) avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato. L'autenticazione della **firma elettronica**, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di **firma elettronica avanzata** consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico. 3. L'apposizione della **firma digitale** da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2. 4. Se al **documento informatico** autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23.

Il servizio è riservato agli utenti registrati

Iscriviti
Sei già registrato? **Accedi**

Il servizio è riservato agli utenti registrati

Iscriviti
Sei già registrato? **Accedi**