

IL DIRITTO DEGLI AFFARI

Fasc. 2 – 2025

ANDREA GRAZIOSI

BREVI CONSIDERAZIONI SULL'EFFICACIA PROBATORIA DEL DOCUMENTO INFORMATICO IN AMBITO EUROPEO

Estratto

ISSN 2281-4531



BREVI CONSIDERAZIONI SULL'EFFICACIA PROBATORIA DEL DOCUMENTO INFORMATICO IN AMBITO EUROPEO*

ANDREA GRAZIOSI
Professore ordinario
nell'Università di Ferrara

SOMMARIO: 1. Introduzione. – 2. Le normative nazionali. – 2.1. Quella italiana. – 2.2. francese. – 2.3. tedesca. – 2.4. inglese. – 3. Qualche spunto comparatistico. – 4. Criticità e prospettive future. – 5. Conclusioni.

1. – Nel contesto della progressiva e sempre più massiccia digitalizzazione dei sistemi giudiziari di tutti i Paesi dell'Unione europea, il documento informatico – definito a livello europeo un po' genericamente come «*qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva*»¹ – ha assunto, com'è ovvio, un ruolo centrale nella dinamica dell'istruzione probatoria di ogni processo civile europeo.

L'ordinamento UE ha già da tempo delineato un proprio quadro normativo di riferimento per garantire la validità transnazionale di tali documenti e delle relative firme elettroniche, nel quale oggi campeggia principalmente il Regolamento (UE) n. 910/2014 (*Regolamento europeo per l'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno* – abbreviato in *eIDAS*, acronimo di *electronic IDentification, Authentication and trust Services*) che ha sostituito la precedente direttiva 1999/93/CE.

Esso stabilisce in primo luogo che un documento o una firma in formato elettronico non possa essere discriminato quanto ad effetti giuridici ed

* Questo scritto è destinato agli Studi in onore di Paolo Biavati.

¹ Così si esprime l'art. 3, n. 35 del Reg. UE, n. 910/14, cd. *eIDAS*; sul concetto e sulla problematica definizione del documento informatico sia consentito il rinvio a GRAZIOSI, *Premesse ad una teoria probatoria del documento informatico*, in *Riv. trim. dir. proc. civ.*, 1998, 492; nonché per maggiori approfondimenti e richiami bibliografici, anche a ID., *La nuova efficacia probatoria del documento informatico*, in *Riv. trim. dir. proc. civ.*, 2003, 53 ss.; ID., voce *Documento informatico (dir. proc. civ.)*, in *Enc. dir.*, Annali, II, Milano, 2008, 492 ss.; ID., *Parola detta, parola scritta e parola telematica, questioni in tema di prova e provenienza*, in *Scrittura e diritto, Quaderni Riv. trim. dir. proc. civ.*, 3, Milano, 2000, 163 ss.

ammissibilità come prova solo per via della sua forma digitale. In particolare, l'art. 25 stabilisce testualmente che «*un documento o una firma elettronica non possono essere privati di efficacia giuridica e probatoria per il solo fatto della loro forma elettronica*»; inoltre il Regolamento è chiaro nell'attribuire alla *firma elettronica qualificata* la stessa efficacia giuridica di una firma autografa e nell'imporre il riconoscimento reciproco delle firme qualificate tra Stati membri.

Infine, eIDAS disciplina altri aspetti rilevanti in ambito probatorio, ad esempio quello dei sigilli elettronici (che attestano l'origine e l'integrità di un documento emesso da persona giuridica) e quello delle marche temporali qualificate, che godono della presunzione di veridicità della data e ora di formazione del documento, nonché di integrità dei dati associati.

Su questa base comune europea gli ordinamenti interni hanno iniziato ad adeguare le proprie norme nazionali, processuali e sostanziali, pur mantenendo le loro inevitabili specificità.

Di seguito, si cercherà di inquadrare brevemente l'attuale efficacia probatoria del documento informatico nel processo civile in Italia, Francia, Germania e Inghilterra sulla base delle rispettive norme interne, della giurisprudenza e degli orientamenti dottrinali, per poi provare a comparare similitudini e differenze, ed evidenziare criticità e prospettive future verso un'auspicabile armonizzazione europea.

2. – Con tali intenti, possiamo dunque senza indugi alla disamina delle varie normative nazionali di settore che qui si vorrebbe esaminare comparativamente.

2.1 – In Italia la materia è regolata dal *Codice dell'amministrazione digitale* (D.lgs. 82/2005, CAD) e dalle norme del codice civile e di procedura civile in tema di prove.

L'art. 20 CAD, in particolare, disciplina la "*Validità ed efficacia probatoria dei documenti informatici*" e distingue sostanzialmente due tipologie di documento informatico digitalmente sottoscritto, prevedendo che:

- se esso è dotato di una *firma elettronica qualificata o digitale* (o altra firma elettronica avanzata) oppure è formato tramite un processo che garantisca l'identificazione informatica dell'autore, sicurezza, integrità e immutabilità, allora soddisfa il requisito della forma scritta ed ha l'efficacia della scrittura privata *ex art. 2702 c.c.*; in altre parole, un documento informatico così sottoscritto è equiparato ad un documento cartaceo firmato di pugno dal suo autore e fa piena prova fino a querela di falso della

provenienza delle dichiarazioni da chi l'ha sottoscritto ai sensi dell'art. 2702 c.c.;

- in tutti gli altri casi – ad esempio e.mail ordinarie, SMS, messaggi sui *social network* privi di firme digitali – la validità come “forma scritta” ed il valore probatorio del documento sono liberamente valutati dal giudice, tenuto conto, comunque, di caratteristiche quali sicurezza, integrità e immodificabilità; ciò non significa che tali documenti “semplici” siano privi di efficacia probatoria, poiché la giurisprudenza italiana ha recentemente chiarito che anche SMS ed e.mail non firmati digitalmente rientrano tra le riproduzioni informatiche di cui all'art. 2712 c.c. e fanno piena prova del loro contenuto se la controparte non ne contesta la conformità ai fatti rappresentati; in caso di contestazione specifica sulla veridicità della riproduzione, il giudice può comunque accertarne la genuinità con altri mezzi di prova, ivi comprese presunzioni².

Ulteriori disposizioni del CAD consolidano l'affidabilità probatoria del documento informatico, e così, ad esempio, l'art. 20, comma 1-*ter* prevede la presunzione di riconducibilità al titolare della firma digitale delle operazioni effettuate col suo dispositivo di firma, salvo prova contraria; inoltre, specifiche regole tecniche (Linee guida AgID) disciplinano la formazione, conservazione ed esibizione dei documenti digitali, prevedendo che la mancata conformità a tali regole possa far perdere al documento l'efficacia probatoria privilegiata.

Da ultimo, va ricordato che il c.p.c. e la normativa sul cd. Processo Civile Telematico (P.C.T.) prevedono che gli atti e documenti in formato elettronico,

² La Suprema Corte ha confermato tali principi, equiparando appunto l'SMS o l'e-mail non firmata ad una rappresentazione meccanica *ex art.* 2712 c.c., ad esempio in Cass., 17 luglio 2019, n. 19155, secondo cui «L'sms contiene la rappresentazione di atti, fatti o dati giuridicamente rilevanti ed è riconducibile nell'ambito dell'art. 2712 c.c., con la conseguenza che forma piena prova dei fatti e delle cose rappresentate se colui contro il quale viene prodotto non ne contesta la conformità ai fatti o alle cose medesime; tuttavia, l'eventuale disconoscimento di tale conformità non ha gli stessi effetti di quello della scrittura privata previsto dall'art. 215, 2° comma, c.p.c., poiché, mentre, nel secondo caso, in mancanza di richiesta di verifica e di esito positivo della stessa, la scrittura non può essere utilizzata, nel primo non può escludersi che il giudice possa accertare la rispondenza all'originale anche attraverso altri mezzi di prova, comprese le presunzioni; ciò posto, va affermato che non è sufficiente una generica contestazione atteso che il disconoscimento, da effettuare nel rispetto delle preclusioni processuali, deve essere chiaro, circostanziato ed esplicito e concretizzarsi nell'allegazione di elementi attestanti la non corrispondenza tra la realtà fattuale e quella riprodotta»; conf. v. anche Cass., 21 febbraio 2019, n. 5141.

sottoscritti digitalmente e depositati tramite PEC, siano validamente prodotti in giudizio, purché ciò avvenga nel rispetto dei requisiti e delle forme telematiche stabiliti dalla legge³.

In sostanza, quindi, in Italia si è delineato un regime probatorio duale: documenti informatici “forti” (firmati digitalmente o con requisiti CAD) con valore di piena prova legale, e documenti informatici “semplici” soggetti al prudente apprezzamento del giudice, sebbene questi ultimi possano ugualmente condurre alla prova dei fatti di causa in mancanza di contestazioni specifiche⁴.

2.2. – L’ordinamento francese già con la *Loi du 13 mars 2000* ha modificato il *Code civil* per riconoscere all’*écrit électronique* dignità probatoria pari a quella degli atti cartacei.

Oggi le disposizioni chiave si trovano negli artt. 1366 e 1367 c.c.:

- l’art. 1366 c.c. stabilisce in particolare che *«l’écrit électronique a la même force probante que l’écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu’il soit établi et conservé dans des conditions de nature à en garantir l’intégrité»*; dunque, per avere pieno valore di prova scritta, un documento elettronico deve assicurare l’identificazione certa dell’autore e la sua integrità;

- l’art. 1367 c.c. prevede, a sua volta, che *«La signature nécessaire à la perfection d’un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l’authenticité à l’acte.*

Lorsqu’elle est électronique, elle consiste en l’usage d’un procédé fiable d’identification garantissant son lien avec l’acte auquel elle s’attache. La fiabilité de ce procédé est présumée, jusqu’à preuve contraire, lorsque la signature électronique est créée, l’identité du signataire assurée et l’intégrité de l’acte garantie, dans des conditions fixées par décret en Conseil d’Etat»; la norma considera perciò “signature” necessaria alla validità di un atto giuridico il mezzo che identifica il suo autore e rende manifesto il suo consenso, precisando che quando è

³ Sul cd. P.C.T., divenuto ormai l’unica forma di trattazione del processo civile in Italia, sia consentito il rinvio, anche per i necessari richiami bibliografici, a GRAZIOSI, *Giurisdizione civile e nuove tecnologie*, I – *Il processo civile telematico*, in *Giusto proc. civ.*, 2024, p. 37 ss.

⁴ Per alcune notazioni critiche su questo sistema, ed in particolare sul valore di prova legale attribuito *ex lege* alle cd. firme forti, sia consentito il rinvio a GRAZIOSI, *Giurisdizione civile e nuove tecnologie*, cit., p. 55 ss.

“*électronique*”, la firma consiste nell’uso di un procedimento affidabile di identificazione che garantisca il collegamento della firma all’atto cui essa si riferisce.

In sostanza, il legislatore francese ha adottato un approccio tecnologicamente neutro, basato su criteri di affidabilità ed efficienza: non viene richiesto uno specifico tipo di firma, ma se il metodo elettronico impiegato è “*fiable*” e assicura integrità, l’equivalenza con la scrittura tradizionale è sicuramente possibile e completa; si può quindi registrare una evidente convergenza con i requisiti delle firme elettroniche avanzate e qualificate definiti da eIDAS, tant’è vero che la dottrina francese tende a ritenere che le norme del *Code civil* siano sostanzialmente allineate al Regolamento UE.

In ambito processuale, va osservato che se per un verso il *Code de procédure civile* consente l’utilizzo di copie o riproduzioni elettroniche - ad esempio, una *copie numérisée* di un atto può valere come prova, salva la facoltà di chi la contesta di chiedere l’esibizione dell’originale - per altro verso vige in generale nel processo civile francese il principio della *liberté de la preuve* nei fatti giuridici, sicché per provare un fatto materiale è solitamente ammesso qualsiasi mezzo di prova (e perciò anche SMS, email o fotografie digitali).

Viceversa, per gli *actes juridiques* (dichiarazioni negoziali) di valore superiore ad € 1500, la legge richiede una prova scritta “*preconstituée*” (art. 1359 c.c), ma essa può essere costituita anche dall’*écrit électronique* se rispetta le condizioni di identificazione e *intégrité* di cui al sopra richiamato art. 1366.

La giurisprudenza francese è solitamente ben allineata su tali principi, e così, ad esempio, la *Cour de cassation* ritiene che un *contrat* può validamente risultare da uno scambio di e-mail, pur distribuite su più messaggi, purché da esse si possa ricavare con sufficiente affidabilità l’*accord des parties* (in tale giurisprudenza viene sottolineato che nell’era digitale non si può pretendere un unico documento informatico contenente tutte le firme, potendo il contratto perfezionarsi anche attraverso più corrispondenze elettroniche⁵).

Quanto alla firma digitale qualificata, la Francia - recependo eIDAS - la considera una modalità tipica per raggiungere l’affidabilità probatoria richiesta dalla sua normativa interna, in quanto l’uso di una *signature électronique qualifiée* conforme al regolamento UE garantisce *ex lege*

⁵ In un caso del 2020, la *Cour de cassation* ha addirittura affermato che un *échange de courriels* (e.mail) soddisfaceva il requisito di forma scritta *ad substantiam* previsto dal *Code du sport*, richiamando il principio secondo cui occorre guardare al *contenuto e alla sostanza dell’accordo*, anziché al supporto delle dichiarazioni negoziali.

l'identificazione dell'autore e l'integrità del documento e perciò un documento così firmato gode *ipso iure* della stessa forza probante di una scrittura privata con sottoscrizione autenticata.

In sintesi, nell'ordinamento francese il documento informatico ha piena validità di *preuve littérale* se sono rispettati i requisiti di identificazione ed integrità (generalmente assicurati mediante firme elettroniche certificate), mentre in caso contrario esso potrà comunque valere come *indice* o *commencement de preuve*, la cui efficacia è lasciata alla libera valutazione giudiziale caso per caso.

2.3. – Il diritto tedesco, tradizionalmente molto formale in materia di documenti e firme, ha in realtà recepito precocemente il riconoscimento del documento elettronico attraverso modifiche al *Bürgerliches Gesetzbuch* (BGB) e alla *Zivilprozessordnung* (ZPO).

Sul piano sostanziale il §126a BGB ammette che la forma scritta richiesta dalla legge possa essere soddisfatta anche dalla firma elettronica qualificata, stabilendo che se una disposizione richiede la forma scritta (*schriftform*), questa è rispettata anche apponendo al documento elettronico il nome del dichiarante ed una *signatur elektronische qualifiziert*, salvo eccezioni espressamente previste dalla legge (ad es. in materia di diritto successorio o familiare, dove l'uso di firma elettronica è vietato).

Ciò garantisce parità di trattamento, ai fini della validità degli atti e dei negozi giuridici, tra documento con firma autografa e documento sottoscritto con *qualifizierte elektronische Signatur* (QES).

Dal punto di vista processuale, la ZPO contiene una norma *ad hoc*, il §371a ZPO, intitolato "*Beweiskraft elektronischer Dokumente*" (efficacia probatoria dei documenti elettronici), ove si stabilisce che ai documenti informatici privati muniti di firma elettronica qualificata si applicano le stesse regole sull'efficacia probatoria delle scritture private cartacee. In sostanza, un file digitale sottoscritto con QES è equiparato a una *Privaturkunde* con firma autografa che, secondo il §416 ZPO, fa piena prova fino a querela di falso della provenienza della dichiarazione dal sottoscrittore. Si delinea così una presunzione di autenticità a favore del documento informatico sottoscritto con firma elettronica qualificata che, se conforme all'art. 32 eIDAS, offre una *cd. prima facie evidence* dell'autenticità della dichiarazione elettronica, superabile solo da una qualificata prova contraria fondata su fatti che facciano legittimamente dubitare che la dichiarazione provenga effettivamente dal titolare della firma (sul punto, la dottrina tedesca si appella ad "una elevata

soglia di contestazione”, cioè fatti che gettino suscitino “gravi dubbi” sulla attribuzione della firma al soggetto che appare come il sottoscrittore).

Naturalmente anche la ZPO (§130a) consente il deposito telematico degli atti processuali firmati digitalmente, a condizione che soddisfino i requisiti formali fissati dalla legge per la sottoscrizione degli atti giudiziari.

In definitiva, in Germania vige un impianto normativo che conferisce al documento elettronico con QES piena efficacia di prova legale, del tutto paragonabile a quella di un documento cartaceo con firma autografa (*Unterrichtungsbroschüre Elektronische Signaturen*); se invece il documento informatico è privo di firma qualificata, non gode di *Beweiskraft ex §371a* e sarà trattato come *Augenscheinsbeweis* (prova libera) ai sensi dei §§371 e 286 ZPO, il che significa che il giudice ne valuterà liberamente il valore probatorio nell’ambito del principio del *freies Beweiswürdigung* (libero apprezzamento delle prove).

Di talché anche l’ordinamento tedesco, analogamente a quello italiano, distingue tra documenti informatici “qualificati” – che soddisfano stringenti criteri formali e godono di presunzioni di autenticità – e documenti elettronici semplici, utilizzabili come mezzi di prova, ma privi di un’efficacia probatoria tipica e predeterminata dalla legge.

2.4 – Nel sistema inglese di *common law* non esiste una codificazione organica dell’efficacia probatoria dei documenti informatici paragonabile a quella che si riscontra nei codici civili e/o processuali di area continentale; tuttavia, con l’evoluzione giurisprudenziale e con alcuni interventi legislativi mirati è stata raggiunta, nella pratica, una sostanziale equiparazione con i sistemi di *civil law*.

Un pilastro di questo progressivo allineamento è rappresentato dal *Civil Evidence Act* del 1995, che ha rivoluzionato le regole sulla prova documentale in sede civile. L’*Act* ha abolito il divieto di ammissione della *hearsay evidence* (letteralmente “per sentito dire”, in sostanza le cd. prove *de relato*) nei procedimenti civili, consentendo quindi che le dichiarazioni contenute in documenti (anche elettronici) possano essere utilizzate come prova di una dichiarazione di scienza o di volontà senza necessità che l’autore testimoni personalmente in giudizio sulla loro conformità al vero. Ciò ha consentito di superare le vecchie restrizioni che gravavano, ad esempio, sulle registrazioni informatiche: prima occorreva dimostrare il funzionamento regolare del computer (secondo il *Police and Criminal Evidence Act 1984* e precedenti normative), mentre dal 1995 in poi la legge presume veritieri i cd. record

digitali d'azienda ed altri documenti elettronici, demandando al giudice la valutazione caso per caso della loro effettiva efficacia probatoria.

Il *Civil Evidence Act* semplifica, inoltre, l'utilizzazione di documenti contenuti in un computer, giacché la sezione 8 consente la copia di tali documenti come prova documentale, subordinandone l'autenticazione di conformità a modalità ritenute adeguate dal giudice. In altre parole, la copia di un documento elettronico può essere utilizzata in giudizio senza ulteriori formalità, e solo in caso contestazione sull'autenticità è richiesto alla parte che vuole avvalersene di provare la conformità all'originale.

Parallelamente, il legislatore ha affrontato *ex professo* il tema della firma elettronica con l'*Electronic Communications Act 2000* (ECA 2000), nella cui Sezione 7 si dispone che un'autenticazione elettronica apposta o associata ad un documento informatico "è ammissibile come prova" dell'autenticità e/o dell'integrità del documento stesso.

In pratica, la validità probatoria della firma digitale trova espresso riconoscimento, posto che un documento firmato elettronicamente può essere prodotto in giudizio e la firma costituirà *evidence* immediata dell'autenticità e/o non alterazione del documento. Eppure, va sottolineato che tale normativa di *common law* (ECA 2000) non crea una vera e propria presunzione legale di equivalenza tra firma digitale e firma olografa, ma garantisce semplicemente che la firma elettronica sia ammessa come mezzo di prova e che pertanto possa essere valutata dal giudice per attestare l'autenticità e/o l'integrità del documento; e così, in assenza di contrasti tra le parti una firma digitale potrà costituire prova della provenienza del documento dal suo autore, se invece vi è contestazione (ad esempio si sostiene che la firma sia stata apposta da terzi non autorizzati e sia stata falsificata), il giudice valuterà le risultanze tecniche disponibili (certificati, *audit trail*, ecc.) e deciderà in merito alla genuinità della firma.

Va aggiunto che la prassi giudiziaria inglese, pur senza attingere a categorie formali, come quella di "firma qualificata", proprie del diritto continentale, ha maturato orientamenti molto flessibili e pragmatici, che hanno condotto, ad esempio, alcuni tribunali a ritenere valide come firme il nome digitato in calce ad una e.mail, o perfino la firma inserita automaticamente come *footer* nelle e.mail (nel caso di specie al fine di soddisfare i requisiti di "*writing and signature*" richiesti da talune leggi speciali come il *Law of property Act* del 1925).

Nel 2019 una dichiarazione congiunta della *Law Commission* e del Governo britannico ha confermato ufficialmente che nel diritto inglese «le firme elettroniche sono valide e legalmente efficaci per sottoscrivere documenti, inclusi

contratti, garantendo l'intenzione di autenticarne la provenienza», sgombrando così il campo da eventuali dubbi residui sulla “tenuta probatoria” delle firme digitali nei casi in cui la legge richiede la firma scritta.

In sintesi, l'approccio inglese al problema dell'efficacia probatoria del documento informatico si basa su due cardini fondamentali: la libera ammissibilità di queste prove – grazie all'abolizione della *hearsay rule* qualsiasi supporto elettronico rilevante è tendenzialmente ammissibile – unita alla flessibilità nella loro valutazione, poiché qualsiasi metodo di firma o attestazione elettronica capace di identificare l'autore può essere considerato una firma agli effetti di legge e comunque sarà considerato dal giudice come indizio probante della provenienza del documento.

Ciò riflette, invero, la filosofia di fondo del *common law* tendente a privilegiare sempre la sostanza (qui l'effettiva intenzione delle parti e l'attendibilità delle circostanze di fatto allegare dalle parti a riprova) sulla forma, pur senza ignorare l'indiscutibile importanza delle garanzie tecniche di integrità ed autenticità dei documenti informatici.

3. – Dalla breve analisi sin qui svolta, emerge che tutte le giurisdizioni considerate riconoscono ormai al documento informatico una piena dignità probatoria nel processo civile, sebbene con approcci normativi diversi figli delle rispettive tradizioni storico-giuridiche.

Una prima importante analogia tra i vari sistemi è l'influenza del quadro normativo delineatosi in sede UE: Italia, Francia e Germania hanno recepito i principi di eIDAS nei propri ordinamenti, attribuendo alle firme elettroniche qualificate (o comunque ai documenti digitali considerati affidabili) lo stesso valore legale della firma autografa. In Italia e Germania ciò avviene tramite espresse equiparazioni normative (art. 20 CAD; § 371a ZPO) che conferiscono al documento informatico firmato digitalmente l'efficacia probatoria tipica della scrittura privata. La Francia adotta invero una formula normativa più generica ma equivalente, poiché subordina detta equiparazione alla concreta identificabilità dell'autore ed integrità informatica del documento (art. 1366 c.c.), requisiti, questi, che solitamente sono pienamente soddisfatti dall'uso di certificati di firma digitale omologati e tecnicamente affidabili. L'Inghilterra, pur non avendo una disposizione di legge che parifichi formalmente il documento elettronico a quello cartaceo, di fatto consegue lo stesso risultato tramite la combinazione di leggi permissive in tal senso (ECA 2000, CEA 1995) ed una *case law* ormai consolidata, ed infatti, come si è visto, la prova documentale di un contratto può basarsi tanto su firme elettroniche che su firme olografe, fatta salva in entrambi i casi la facoltà

per la parte contro cui è prodotto il contratto contestare l'autenticità della propria sottoscrizione, fornendo adeguata prova contraria in tal senso.

Un altro elemento di comunanza è dato dalla constatazione che ovunque viene adeguatamente assicurata la facoltà di opposizione alla parte che contesta la genuinità di un documento informatico e della sua sottoscrizione digitale (ad esempio ne nega la provenienza o lamenta alterazioni). In Italia ciò avviene, come visto, sia tramite il meccanismo del disconoscimento della riproduzioni meccaniche *ex art. 2712 c.c.*, sia tramite il più complesso procedimento di verifica della scrittura privata *ex art. 216 c.p.c.* per le firme digitali contestate; in Francia il giudice può ordinare una consulenza tecnica sul documento informatico oggetto di contestazione (artt. 287 ss. c.p.c.) e così pure può fare il giudice tedesco su firme o certificati non riconosciuti; in Inghilterra, parimenti, si può ricorrere a *expert evidence* (ad es. un perito informatico) per valutare l'autenticità delle produzioni informatiche.

D'altro canto, permangono ancora anche differenze significative. Tra queste la più cospicua concerne il concetto e l'efficacia giuridica di prova legale conosciuti solo dai sistemi continentali di *civil law*, ma non da quelli di *common law*, e valevole per taluni documenti. E così, ad esempio, in Italia e Germania gli atti pubblici e le scritture private con sottoscrizione autenticata (anche in forma digitale qualificata) fanno piena prova fino a querela di falso, mentre nei sistemi di *common law* la prova documentale rientra sempre nel libero apprezzamento del giudice senza distinzioni di sorta tra differenti categorie di prove. Ne discende che negli ordinamenti continentali la sottoscrizione autenticata tradizionale o la (equipollente) firma elettronica qualificata sono entrambe assistite da una presunzione di autenticità superabile solo tramite specifici dispositivi di contestazione (in Italia la querela di falso), mentre in Inghilterra il giudice valuta semplicemente se la contestazione avversaria genera "ragionevoli dubbi" sull'affidabilità del file o della firma.

Un'altra non trascurabile differenza concerne i requisiti formali di firma originari, poiché negli ordinamenti romano-germanici solo la firma elettronica "forte" (avanzata/qualificata) garantisce l'equipollenza alla firma autografa (art. 20 CAD e *Unterrichtungsbroschüre Elektronische Signaturen*), altrimenti il documento rimane sottoposto al libero apprezzamento del giudice. Del pari in Francia, pur non essendo tipizzati i "gradi" e le tipologie di firma, di fatto l'utilizzo di strumenti qualificati è il modo più sicuro e ricorrente per soddisfare le esigenze di identificazione e integrità richieste dall'art. 1366 c.c. Al contrario, il diritto inglese adotta invece un approccio più flessibile, pragmatico e graduale, posto che ogni firma elettronica "idonea"

(dall'immagine scannerizzata di una firma, al nome digitato, fino alla firma digitale con certificato) può essere ammessa come mezzo di prova e così non esiste una gerarchia formale di tipologie di firma, ma naturalmente all'aumentare dell'affidabilità tecnica crescerà anche la forza persuasiva della prova.

In termini più generali, si può affermare che gli ordinamenti dell'Europa continentale sono generalmente basati su norme di validità formale più rigide – derivanti, tra l'altro, anche dalla possibilità che negli ordinamenti di *civil law* la forma scritta sia richiesta per la validità di certi atti e quindi, per inciso, una loro eventuale dematerializzazione per avere valore giuridico richiede per forza una firma qualificata – mentre il sistema di *common law* è prevalentemente incentrato sulla pertinenza e autenticità delle risultanze istruttorie, trattando la forma come un aspetto tecnico da valutare *ex post*.

Nonostante queste cospicue differenze di fondo, vanno comunque rimarcate le ulteriori linee di convergenza che contraddistinguono quanto settore, posto che tutti gli ordinamenti esaminati ammettono la possibilità di ricorrere a copie digitali di documenti come mezzi di prova: in Italia, una scansione di documento analogico, se conforme alle regole tecniche, ha la stessa efficacia dell'originale (art. 22 CAD); in Francia, la *copie fidèle e durable* di un atto ha forza probante pari all'originale (art. 1379 c.c.); in Germania, il §371b ZPO conferisce a talune copie digitali di atti pubblici piena efficacia probatoria; in Inghilterra, il tradizionale *best evidence rule*, che richiedeva sempre la produzione dell'originale, è stato ormai superato nella prassi, ove la produzione di una copia elettronica è generalmente ammessa, salvo vi sia fondato motivo per dubitare della sua conformità all'originale.

Da questo quadro comparativo sembra emergere, in definitiva, che le differenze residue riguardino più questioni di tecnica giuridica (presunzioni legali vs valutazione libera) che non l'esperienza pratica, visto che in tutti i Paesi europei esaminati un documento informatico tecnicamente affidabile può essere utilizzato per dimostrare i fatti rilevanti nel processo, ed inoltre l'uso di firme elettroniche certificate agevola fortemente il giudizio sulla sua attendibilità, essendo solitamente considerate equipollenti alla sottoscrizione autografa tradizionale.

4. – Nonostante i notevoli progressi compiuti permangono alcune criticità nel processo di uniformazione probatoria nell'utilizzazione dei documenti informatici come mezzo di prova in ambito UE.

Un primo problema è di carattere squisitamente tecnico, giacché un documento informatico per mantenere il suo valore probatorio deve essere

necessariamente conservato in formati e con modalità sicure (ad esempio in Italia la conservazione digitale conforme alle linee guida AgID – Agenzia per l'Italia digitale). La perdita di integrità (come la corruzione del file o la modifica non autorizzata) può ovviamente comprometterne la concreta utilizzabilità nonché l'efficacia probatoria del supporto informatico utilizzato. Questo problema si accentua notevolmente a causa della rapida obsolescenza tecnologica che colpisce qualsiasi strumento informatico: formati, supporti e sistemi di firma elettronica possono diventare antiquati o insicuri col tempo, richiedendo migrazioni e procedure di *resignature* (rinnovo delle firme, marche temporali, ecc..) per mantenere la loro validità nel lungo e medio periodo.

Gli Stati dovranno perciò investire in infrastrutture di archiviazione e verifica adeguamento tecnologico assai robuste, e le normative nazionali dovranno essere costantemente aggiornate per assicurare, ad esempio, l'impiego di algoritmi sicuri e l'aggiornamento delle certificazioni divenute obsolete.

Un secondo profilo critico riguarda la sicurezza e l'affidabilità, poiché se è vero che le firme digitali qualificate sono altamente attendibili sul piano strettamente informatico, è altrettanto vero che in pratica possono essere falsificate. Casi di furto di identità digitale, uso indebito di dispositivi di firma altrui o vulnerabilità dei *software* possono compromettere gravemente l'affidabilità probatoria di un documento apparentemente "firmato" digitalmente. In Italia, ad esempio, vige la presunzione di utilizzo da parte del titolare del dispositivo di firma (Art. 20. CAD), ma questo potrebbe essere foriero di gravi disfunzioni e abusi, nel caso in cui qualcuno si appropri fraudolentemente di un dispositivo di firma altrui⁶. Pertanto, sul piano istruttorio sarà necessario valutare in modo sempre molto rigoroso, non solo l'attendibilità intrinseca del documento, ma anche del processo di firma e delle misure di sicurezza adottate (PIN, smart card, autenticazione multifattoriale, ecc.) e così la cooperazione fra giuristi ed informatici forensi diverrà sempre più essenziale per affrontare eventuali contestazioni sulla genuinità di un documento informatico e sulla firma digitale ad esso apposta.

Un terzo problema è il cd. *digital divide* giudiziario, visto che non tutti gli operatori giudiziari, giudici e avvocati, hanno pari familiarità con gli strumenti digitali e le relative implicazioni probatorie, sicché potrebbero verificarsi ingiustificate difformità applicative tra i vari Fori nell'approccio agli

⁶ Su questo specifico aspetto sia di nuovo consentito il rinvio a GRAZIOSI, *Giurisprudenza civile e nuove tecnologie*, cit., p. 55.

strumenti informatici anche di uso più comune, come ad esempio un semplice *screenshot* o un *log di database* prodotti in giudizio come prova.

Sul fronte delle prospettive future si assiste invece ad una duplice tendenza in ambito UE, da un lato la giurisprudenza dei vari Stati sta meritoriamente evolvendosi al fine di raffinare i preesistenti istituti fondamentali in materia di prove al fine di adattarli alle nuove tipologie di prove digitali (si pensi alle chat di WhatsApp, ai post sui social media, ai dati di geolocalizzazione – tutti elementi che rientrano nella definizione ampia di “documento elettronico” e che già vengono spesso utilizzati come prove nei giudizi civili); dall’altro lato, il legislatore europeo è già attivo nel promuovere un’ulteriore grado di armonizzazione, poiché è in cantiere l’eIDAS 2.0 con una proposta di regolamento che probabilmente rafforzerà le identità digitali europee e potrebbe anche introdurre strumenti come il “*wallet*” digitale per cittadini e imprese; questo potrà ovviamente avere risvolti probatori, poiché un’identità digitale certificata UE renderebbe più agevole l’autenticazione di documenti e contratti online, aumentando la sicurezza degli scambi transfrontalieri.

Da ultimo va osservato che l’UE sta investendo in progetti come *e-CODEX* per interconnettere elettronicamente le autorità giudiziarie, con la conseguenza che in un prossimo futuro le prove digitali potrebbero essere trasmesse da un Paese all’altro attraverso canali standardizzati sicuri, riducendo le possibili contestazioni su validità ed integrità nel passaggio transfrontaliero.

Sul piano comparato permane però la questione di fondo dell’eterogeneità delle norme processuali, giacché l’ammissibilità e la valutazione delle prove nei procedimenti giudiziari sono generalmente considerate come materia di sovranità nazionale di ogni singolo Stato sulla quale l’UE può intervenire solo tangenzialmente. Ciò implica che nonostante eIDAS abbia uniformato l’efficacia esterna delle firme digitali, obbligando gli Stati a riconoscere la validità di una firma digitale straniera, l’apprezzamento interno di queste prove continuerà a poter differire. E così, ad esempio, se un documento elettronico con firma qualificata italiana ha libero ingresso in un processo civile tedesco con la medesima efficacia probatoria, resta aperta la possibilità che i due ordinamenti abbiano regole diverse su come il giudice debba procedere alla sua valutazione in caso di contestazione.

Nel lungo periodo, la prospettiva auspicata da tutti gli osservatori è di una maggiore convergenza anche a livello di culture probatorie, che dovrebbe essere facilitata nel tempo, poiché man mano che l’uso dei documenti informatici diventerà la norma tra gli operatori economici (si pensi ai contratti

“nativamente” elettronici, senza equivalente cartaceo), i vari sistemi giuridici tenderanno necessariamente ad allinearsi nel dare fiducia a tali documenti, pena, altrimenti, l'impossibilità di far valere in giudizio una sempre più vasta gamma di diritti in un contesto ormai altamente dematerializzato.

5. – In conclusione, l'efficacia probatoria del documento informatico nel processo civile è oggi pacificamente riconosciuta in tutta l'Unione Europea ed è frutto del concorso tra innovazione normativa ed adattamento interpretativo dei principi tradizionali in materia di prova. Il quadro comune europeo, plasmato dal Regolamento eIDAS e dai sempre nuovi prodotti che si affacciano sul mercato digitale, ha favorito l'adozione di standard condivisi, quali la non discriminazione del documento elettronico rispetto alla carta, l'equiparazione della firma digitale qualificata alla firma autografa, il mutuo riconoscimento transfrontaliero delle identità e delle firme digitali, che oggi rappresentano ormai punti fermi.

Gli ordinamenti nazionali di Italia, Francia, Germania e Inghilterra, pur con soluzioni tecniche diverse, appaiono convergenti nel riconoscere valore di prova piena al documento informatico quando questo presenti adeguate garanzie di autenticità e integrità.

Le differenze permangono, invece, – più marcate tra *common law* e *civil law* – sulle modalità procedurali di contestazione e sul grado di formalizzazione richiesto *ex ante* per attribuire valore legale alla prova. Tali differenze tuttavia si stanno attenuando di fronte alla progressiva digitalizzazione del processo civile in ogni sistema processuale, basti solo pensare che in tutti i Paesi esaminati i processi civili vedono ormai una sempre più diffusa la gestione elettronica degli atti processuali e la trattazione digitale e telematica della causa, al punto che ormai si assiste ad una sorta di armonizzazione di fatto che precede quella di diritto.

Ciò non toglie che vi sia margine e necessità per interventi futuri tesi ad assicurare un diritto probatorio digitale sempre più uniforme in ambito UE, e tale obiettivo andrebbe probabilmente perseguito con linee guida sovranazionali ed un rafforzamento del dialogo tra Corti supreme sui principi fondamentali da porre a base dei vari sistemi.

In definitiva, il *trend* è sicuramente verso un sistema probatorio sempre più in sintonia con l'ecosistema digitale, ove il documento informatico non è più visto come un'eccezione da tollerare, ma come la forma ordinaria di prova documentale, con la conseguenza che la sfida futura diventerà semmai quella inversa per dare ai pochi documenti analogici ancora rimasti un'adeguata disciplina e collocazione processuale.

L'auspicio conclusivo è insomma che, attraverso il dialogo tra legislazione UE e riforme interne, si realizzi un contesto di piena fiducia reciproca sul valore dei documenti informatici, consolidando così un diritto probatorio europeo capace di garantire efficienza, rapidità ed effettività ai processi civili europei dell'era digitale.

Abstract

BRIEF CONSIDERATIONS ON THE EVIDENTIARY VALUE OF ELECTRONIC DOCUMENTS IN THE EUROPEAN CONTEXT.

L'articolo propone un'indagine comparatistica in ambito europeo sull'efficacia probatoria del documento informatico e della firma digitale nel processo civile, fondandosi prevalentemente sui principi e sulle norme eurounitarie fissati dal Regolamento UE n. 910/2014, denominato eIDAS.

Vengono succintamente presi in considerazione gli ordinamenti giuridici di Italia, Francia, Germania ed Inghilterra al fine di sondarne il grado di reciproca armonizzazione e le prospettive di future evoluzioni verso la piena integrazione tra i Paesi UE, con riguardo alla disciplina processuale di un mezzo di prova destinato ad assumere un ruolo sempre più nevralgico nel quadro della progressiva ed incessante digitalizzazione di tutti i sistemi giudiziari europei.

Nel testo vengono inoltre suggeriti alcuni spunti ricostruttivi che possano favorire l'armonizzazione probatoria dei processi civili europei in un settore, come quello informatico, da cui dipenderà in modo determinante lo sviluppo economico e la competitività di ogni sistema-paese.

The article aims to achieve a comparative investigation in the European context on the evidentiary efficacy of computerised documents and digital signatures in civil proceedings, basing itself mainly on the European principles and rules established by EU Regulation No. 910/2014, known as eIDAS.

The legal systems of Italy, France, Germany and England are briefly taken into consideration in order to sound out the degree of mutual harmonisation and the prospects of future developments towards full integration between EU countries, with regard to the procedural regulation of a means of evidence destined to take on an increasingly crucial role in the framework of the progressive and incessant digitalisation of all European judicial systems.

The text also suggests some reconstructive ideas that may favour the evidentiary harmonisation of European civil trials in a sector, such as the IT sector, on which the economic development and competitiveness of each country-system will depend in a decisive way.
