Digeat N.6 - 19 Giugno 2025

L’autenticità garante di certezza e sostenibilità dei documenti elettronici

Di Fabrizio Lupone

Abstract

L’autenticità è più che mai il *primus* fattore abilitante per garantire l’affidabilità negli ambienti digitali, requisito basico per uno sviluppo economico, sociale e sostenibile. La sensazione di certezza giuridica e sicurezza abilita l’utilizzo diffuso delle transazioni e dei servizi digitali e migliora l’esperienza d’uso degli utenti, permettendo di costruire un mercato unico digitale in Europa di cui fidarsi.

Indice

L’esigenza di autenticità già dall’epoca antica

La storia e l’economia ci insegnano che nelle transazioni e, in generale, nelle relazioni tra persone, tra operatori economici e tra Stati c’è sempre stato bisogno di una **garanzia tra le parti**, che si sostanzia nel fatto che le parti hanno l’esigenza di percepire **un grado di fiducia e sicurezza** che può essere più o meno robusto a seconda della natura e della rischiosità della transazione.

Gli oggetti che spesso hanno rappresentato nel tempo le transazioni e le relazioni tra persone fisiche e giuridiche sono stati i **documenti**, che già dai tempi dell’antichità **richiedevano che ci fosse la garanzia di autenticità** contro il rischio di falsificazioni oppure soltanto per l’esigenza di individuare in modo certo l’autore o le parti in un accordo.

Fin dai tempi del periodo tardo repubblicano e imperiale romano l’autenticità dei documenti doveva essere garantita e tale garanzia era assicurata tramite la catalogazione e la conservazione dei documenti in un edificio dedicato, il ***Tabularium***, costruito da Quinto Lutazio Catulo nel 78 a.C. sul Campidoglio. Chi si occupava di garantire l’autenticità dei documenti e, quindi, di assicurare la **fiducia (*trust*)** alle transazioni del tempo era il ***magister census***, un supervisore che coordinava i lavori di archiviazione e catalogazione nel *Tabularium*.

> Ritornando ai tempi attuali nell’era dell’intelligenza artificiale, dove il concetto di documento elettronico è molto esteso ed è spesso rappresentato da **un insieme di dati digitali di rilevanza giuridica**, anche complesso, le transazioni elettroniche richiedono sempre più **fiducia e responsabilità** visti i rischi di sicurezza, di frodi e

> falsificazioni con il progredire delle tecnologie e della potenza di calcolo. In tale contesto di complessi ecosistemi digitali, la garanzia della fiducia per gli attori coinvolti nelle transazioni è assicurata dall'adozione di **strumenti e servizi digitali fiduciari** e dall'adozione di un modello organizzativo con ruoli e responsabilità.

Come nel passato il magister census deteneva la responsabilità sulla garanzia dell'autenticità dei documenti, oggi i prestatori di servizi fiduciari e i vari Responsabili previsti dalle norme, quali a titolo di esempio il Responsabile della Conservazione, il Responsabile per la protezione dei dati personali, il Responsabile della gestione, il Responsabile della Sicurezza **hanno l'onere e l'onore** di assicurare il valore dell'autenticità ai documenti, ai dati digitali e in senso esteso alle transazioni elettroniche.

Oggi più che mai è necessario garantire l'autenticità

Garantire **l'autenticità** alle transazioni elettroniche e, quindi, agli oggetti che la caratterizzano come i documenti elettronici significa garantire la caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione e che è stato effettivamente **prodotto dalla fonte dichiarata** (requisito del non ripudio).

> Pertanto, **un oggetto digitale è autentico** se nel contempo è integro, completo ed è **non ripudiabile**, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata ed essendo riconducibile all'autore. L'autenticità, pertanto, deve poter essere valutata sulla base di **precise evidenze** che permettono di dimostrare, anche a terzi, l'affidabilità e la paternità del documento o della transazione elettronica.

In Europa e in Italia, la disciplina legislativa che affronta i temi della digitalizzazione dei documenti fornisce i criteri base, le disposizioni e le regole tecniche per implementare processi conformi rispetto alla necessità di **fiducia digitale** richiesta dal contesto.

Del resto, sin dall'antichità, l'affidabilità e l'autenticità di un documento erano **le fondamenta per assicurare la certezza giuridica** e, a maggior ragione oggi, in un mercato ove è forte il rischio di cyberattacchi, di azioni fraudolente e di abuso improprio di strumenti di intelligenza artificiale, **sono diventate un requisito obbligatorio** imposto da una serie di normative comunitarie e nazionali.

Le normative europee ed italiane da anni disciplinano il valore dell'autenticità associato ad un documento elettronico, inteso come *qualsiasi contenuto conservato in forma elettronica che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*.

La normativa vigente disciplina l'autenticità dei documenti informatici

Nel dettaglio, il Regolamento (UE) n. 910/2014, cosiddetto **Regolamento eIDAS** *(Electronic Identification, Authentication and Trust Services)*, è direttamente applicabile in tutti gli Stati Membri UE, senza necessità di atti di recepimento, e ha proprio l'obiettivo di adottare a livello europeo un **quadro tecnico-giuridico unico, omogeneo ed interoperabile** per i documenti elettronici ed i servizi fiduciari qualificati e non, al fine di migliorare in particolare **la fiducia e la sicurezza** delle piccole e medie imprese (PMI) e dei consumatori nell'utilizzo delle transazioni elettroniche nel mercato interno europeo.

Il Regolamento eIDAS, tra le diverse disposizioni, stabilisce che un prestatore di servizi fiduciari qualificato nell'erogazione dei suoi servizi fiduciari qualificati, quali ad esempio le firme o i sigilli

elettronici qualificati, deve utilizzare sistemi affidabili per memorizzare i dati a esso forniti affinché **l'autenticità dei dati sia verificabile.**

> Un documento elettronico è, pertanto, **giuridicamente rilevante se è "autentico"**, vale dire se è riconducibile con certezza alla volontà del suo autore, ricordandosi che si applica sempre il **principio di neutralità della forma** enunciato dallo stesso Regolamento eIDAS, secondo il quale *non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali ad alcun documento elettronico per il solo motivo della sua forma elettronica*.

Nell'ambito dell'ordinamento giuridico nazionale, il valore giuridico e l'efficacia probatoria di un documento elettronico, dalla sua formazione fino alla sua conservazione nella modalità informatica, oggi, sono legittimati da una norma primaria costituita fondamentalmente dal **Codice dell'Amministrazione Digitale** (CAD – Decreto Legislativo 7 marzo 2005, n. 82 s.m.i.) e dal **Codice Civile**, e da norme di riferimento secondarie per ciascun ambito (tributario, lavoristico, civilistico, assicurativo, bancario, ecc.).

Vi è poi un'importante normativa tecnica attuativa, ai sensi dell'art. 71 del CAD, per cui è necessario garantire la conformità, costituita da **regole tecniche e standard** che regolamentano da un lato le regole tecniche sulla fase di formazione, gestione e conservazione dei documenti informatici, con le **Linee Guida AgID**, e dall'altro le regole tecniche sulle firme elettroniche, le validazioni temporali, i dispositivi sicuri per la generazione della firma con il **DPCM 22 febbraio 2013**.

In particolare, quasi a ricordarci che **il requisito di autenticità va preservato per tutta la vita del documento elettronico**, il legislatore nazionale, all'art. 44, comma 1-ter, del CAD dispone che in tutti i casi in cui la legge prescrive obblighi di conservazione, anche a carico di soggetti privati, il sistema di conservazione dei documenti informatici **assicura, per quanto in esso conservato, caratteristiche di autenticità**, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle Linee Guida.

L'autenticità quale asset fondamentale della sicurezza e protezione dei dati personali

In ambito europeo, secondo il Regolamento Generale sulla Protezione dei Dati (UE 2016/679), cosiddetto **GDPR** (*General Data Protection Regulation*), l'autenticità significa assicurare che i dati siano autentici, cioè non falsificati o modificati, e che l'autore di un documento elettronico prodotto o l'utente o il dispositivo che accede ai dati siano effettivamente di chi o cosa dichiarano di essere, al fine di rendere **sicuro, affidabile e riservato il trattamento dei dati personali**.

Con l'entrata in vigore della Direttiva comunitaria 2022/2555, cosiddetta **NIS2**, relativa a misure per un livello comune elevato di sicurezza informatica nell'UE, che in Italia è stata recepita con il **Decreto Legislativo 138/2024**, anche nel percorso di attuazione della Strategia Nazionale di Cybersicurezza è stata aggiunta **l'autenticità come quarto asset fondamentale** per la gestione della cybersicurezza e della continuità del business, oltre a riservatezza, integrità e disponibilità.

> L'autenticità è necessaria per la sicurezza informatica, in quanto permette di assicurare che i dati siano affidabili e che le transazioni siano effettuate con soggetti autentici.

La naturale chiosa dei miei ragionamenti l'affido al **Considerando n. 1) del Regolamento eIDAS**, che correttamente afferma una verità assoluta: "*instaurare la fiducia negli ambienti online è fondamentale per lo sviluppo economico e sociale. La mancanza di fiducia, dovuta in particolare a una percepita assenza di certezza giuridica, scoraggia i consumatori, le imprese e le autorità pubbliche*

dall’effettuare transazioni per via elettronica e dall’adottare nuovi servizi.”

Per tali motivi, tutte le organizzazioni e gli operatori del mercato unico europeo devono garantire, ciascuno per il proprio, il requisito dell’autenticità sui propri documenti, nelle proprie transazioni elettroniche, consapevoli che solo così riusciremo a costruire **un ecosistema digitale davvero *trust***.

Richiesto un approccio sostenibile ESG basato sull’autenticità

> Attraverso i servizi fiduciari e gli strumenti digitali è possibile ottenere oggi una garanzia di certezza giuridica che è pari o anche superiore rispetto a quella dei documenti cartacei, fornendo anche un contributo concreto alla **sostenibilità ambientale, sociale ed economica** *(“Environmental, Social, and Governance – ESG”*).

La necessità di autenticità e, quindi, di credibilità ormai si applica in tutti gli scenari di vita e di lavoro; un esempio calzante sono le strategie di marketing e comunicazione sull’approccio sostenibile degli enti privati e pubblici. La narrazione autentica di progetti e bilanci di sostenibilità di un’organizzazione è alla base della fiducia dei clienti sui prodotti e servizi ricevuti. Il *greenwashing* è un classico esempio di strategia non basata sull’autenticità, trasparenza e dati concreti e deve far riflettere tutti noi, operatori e cittadini, nel coltivare una **cultura di autenticità nella sostenibilità** che possa diventare fattore abilitante dello sviluppo umano e sostenibile.