



Avv. Andrea Lisi

La custodia affidabile del documento informatico nell'era delle nuvole



Contributo edito in
«Revista de Ciencia de la Legislación» n.10
Settembre 2021 (Universidad del Salvador)

Sommario

| | |
|---|----|
| Premesse | 3 |
| L'evoluzione non solo giuridica del documento | 4 |
| La leggerezza (non giuridica) del documento informatico | 5 |
| Le varie tipologie di firma nel mondo digitale | 6 |
| La validità formale e probatoria del documento informatico | 7 |
| L'evoluzione della sottoscrizione nel mondo digitale | 8 |
| Firme elettroniche e articolo 20 CAD | 9 |
| La conservazione dei documenti informatici non si fa in cloud o in blockchain | 10 |
| L' ABC della "digitalizzazione" | 11 |
| La moda passa. La memoria digitale resta. | 11 |
| Le strade praticabili (quelle vere) | 12 |
| La Blockchain: fuori una | 13 |
| Il Cloud: il (dis)orientamento della PA | 13 |
| Conclusioni | 14 |
| Sitografia | 16 |
| Bibliografia essenziale | 16 |

Abstract

Mentre tutto si evolve, inevitabilmente, anche i concetti di formazione, gestione e conservazione del documento non rimangono di certo fermi, assecondando il modificarsi della natura stessa dei documenti con cui abbiamo a che fare. La natura del documento è radicalmente mutata e continua a farlo, forse tanto velocemente che la nostra stessa capacità di concettualizzazione non riesce a starle appresso: il documento moderno, e digitalmente rilevante, non è più solo ciò che di primo acchito la nostra mente assocerebbe a questo nome, ovvero una "carta bollata", una lettera, un certificato, qualcosa che comunque possa esprimersi in una forma cartacea, ma qualcosa di molto più dinamico, strutturato e multicanale, come i flussi di informazioni che vengono scambiati e letti quotidianamente dai sistemi informativi e documentali, sia delle PA che delle organizzazioni aziendali.

Keywords: documento informatico digitalizzazione conservazione cloud blockchain

Premesse

Finalmente oggi, anche in seguito alla terribile situazione pandemica che abbiamo vissuto, siamo maggiormente consapevoli del fatto che il web non sia poi tanto "l'altrove" rispetto alla nostra realtà fisica e che al suo interno coesistano nuovi servizi, che possiamo senz'altro definire ormai "essenziali" nella nostra società, piattaforme, app e strumenti di lavoro a distanza. La possibilità di fruire di tali strumenti implica ben più che la semplice disponibilità di (o meglio accesso a) "infrastrutture digitali", integrando ormai un vero e proprio presupposto per l'esercizio di diritti di cittadinanza digitale, che sono il precipitato di un necessario processo di evoluzione interpretativa alla nostra Carta Costituzionale. Del resto, le attività umane (in ambito pubblicitario, professionale o strettamente privato) si svolgono ormai in buona parte attraverso piattaforme IT e dunque dipendono da esse. E quindi, inevitabilmente, anche l'esercizio dei nostri diritti e libertà fondamentali si esplica attraverso predetti sistemi. Pertanto, proteggere i sistemi e processi IT e custodire correttamente le informazioni inerenti a tali sistemi e processi significa anche tutelare diritti e libertà fondamentali che si dipanano attraverso di essi.

Si fa riferimento non solo ai casi in cui l'accesso a tali piattaforme risulti essere presupposto indefettibile per poter usufruire di un servizio pubblico - come ad esempio nella didattica a distanza che, di fatto, limita la possibilità di garantire a tutti il diritto all'istruzione oppure nella sanità digitale, dove un data breach è in grado di paralizzare un intero sistema di vaccinazione¹ - ma anche alle

¹ Si fa riferimento al data breach subito dalla regione Lazio i primi di agosto 2021 (info utili reperibili da *Attacco hacker alla Regione Lazio: nessun atto terroristico, solo tanta ignoranza informatica*, su Il Fatto Quotidiano, blog di Andrea Lisi reperibile al seguente link <https://www.ilfattoquotidiano.it/2021/08/03/attacco-hacker-alla-regione-lazio-nessun-atto-terroristico-solo-tanta-ignoranza-informatica/6282139/>), dove a distanza di quasi un mese ci sono ancora dati sui vaccini non recuperati (info: *Lazio, senza vaccino 200mila cinquantenni. L'allarme dei medici di famiglia: "Elenchi spariti per l'attacco hacker*, da La Repubblica, reperibile al seguente link

questioni legate ai casi (peraltro già verificatisi) in cui le policy o le scelte del gestore di una piattaforma incidono significativamente proprio sui diritti fondamentali di uguaglianza e libera manifestazione del pensiero. È indispensabile, dunque, interrogarsi sui molteplici impatti giuridici di tali fenomeni, non più ormai in una prospettiva de iure condendo, ma con lo spirito critico e disincantato dell'osservatore che si propone di analizzare – e inquadrare giuridicamente – porzioni di realtà che ci riguardano².

Così è per il documento informatico e per le nuove forme di imputabilità giuridica dal punto di vista digitale, che impattano pesantemente nelle nostre interazioni sociali e nelle nostre dinamiche di acquisto di beni e servizi e in tutti i processi di interazione con soggetti pubblici e privati. Del resto, la quantità di nuove tecnologie che si è dovuto imparare ad adoperare negli ultimi vent'anni a detta di molti esperti non trova eguali in altre fasi della storia dell'umanità. Non è stato possibile accomodarsi troppo a lungo su conoscenze e abitudini acquisite senza che di lì a poco qualcosa cambiasse nuovamente. Solo per fare un esempio che sarà familiare a molti lettori, si è passati nell'arco di poco più di un decennio dal floppy disk al cd, e da questo alla chiave usb e ad altri tipi di supporti portatili di memoria sino alla vertigine dell'"assenza di supporto" per conservare la memoria garantita oggi dall'avvento del cloud computing³.

L'evoluzione non solo giuridica del documento

Mentre tutto si evolve, inevitabilmente, anche i concetti di formazione, gestione e conservazione del documento non rimangono di certo fermi, assecondando il modificarsi della natura stessa dei documenti con cui abbiamo a che fare. Se, infatti, fino agli anni '90 si aveva del document management una visione più ristretta e univoca, che sostanzialmente coincideva con la digitalizzazione di immagini e l'archiviazione ottica di documenti nati originariamente su supporti analogici (prevalentemente cartacei), negli anni 2000 si è passati al concetto già più complesso di "gestione documentale" e "conservazione sostitutiva" e, cioè, la sostituzione del documento cartaceo con l'equivalente documento digitale, il cui contenuto viene "cristallizzato" grazie all'utilizzo della firma digitale e della marca temporale⁴. Oggi oramai ci confrontiamo con processi sempre più nativamente digitali, dove dell'immagine della carta non c'è più traccia.

Insomma, la natura del documento è radicalmente mutata e continua a farlo, forse tanto velocemente che la nostra stessa capacità di concettualizzazione non riesce a starle appresso⁵.

https://roma.repubblica.it/cronaca/2021/08/22/news/senza_vaccino_200mila_cinquantenni_elenchi_spariti_per_l_attacco_hacker_-_314846978/.

² Su questi temi si consiglia la lettura dell'ottima opera di Giacomo Conti *Lineamenti di diritto delle piattaforme digitali*, Maggioli editore, vol. 1 e 2, 2020-2021.

³ Ci si permette di consigliare, come utile lettura in merito all'evoluzione giuridico-archivistica del documento, *L'evoluzione dei documenti e della memoria nella società digitale*, di Andrea Lisi e Silvia Riezzo, pubblicato su ForumPA, acquisibile alla pagina <https://www.forumpa.it/pa-digitale/evoluzione-dei-documenti-e-della-memoria-nella-societa-digitale/>.

⁴ Garantendone così la sopravvivenza nel tempo come originale "autenticamente" digitale attraverso un sistema di conservazione "a norma".

⁵ Se per esempio si cercano lumi su un'enciclopedia online, si potrebbe riscontrare che per "documento" si intende ancora, in prima analisi, "qualsiasi mezzo, soprattutto grafico, che provi l'esistenza di un fatto,

La leggerezza (non giuridica) del documento informatico

Che cos'è esattamente un documento informatico? Ci si è interrogati tante volte negli ultimi venti anni sulla natura della documentazione affidata ai bit e, come già evidenziato nel 2015⁶, ci possiamo aspettare che la risposta a una domanda del genere possa variare sensibilmente in base al soggetto interrogato e alla sua reale percezione della nuova realtà che stiamo vivendo. Probabilmente, chiedendolo a dei "profani" della materia, in molti, sgranando gli occhi e nascondendo un inevitabile disagio, risponderrebbero ancora oggi erratamente, indicando qualcosa di simile a un file word o a un foglio excel, la cui conservazione potrebbe avvenire, magari, dopo un'opportuna stampa o eseguendo un semplice back up in cloud.

Nella mente di buona parte della popolazione questo concetto ancora oggi è certamente poco chiaro e avvolto da una coltre di nebbia che, ci si augura, una maggiore diffusione di una più approfondita cultura digitale⁷, agevolata da una regolamentazione più specifica in ambito europeo, possa contribuire a dissipare. Ma non è solo nella mente dei semplici cittadini che questa confusione risiede, visto che anche a livello "ufficiale" le definizioni utilizzate per il documento informatico (e per le stesse firme apposte su un documento di natura digitale⁸) si sono modificate nel tempo e con esse la concettualizzazione che le accompagna, anche considerato che si utilizzano tutt'ora terminologie differenti per definire i documenti in ambito giuridico (dove ci sono già differenze di approccio tra ambito civile, penale e amministrativo), diplomatico e archivistico⁹. Le stesse attuali definizioni

l'esattezza o la verità di un'asserzione", e solo qualche accezione più in basso si arriva a contemplare anche il "file contenente testo o immagini, creato con un word processor o con un programma di impaginazione" (così vocabolario Treccani alla pagina <https://www.treccani.it/vocabolario/documento/>) e qui ci si ferma. Anche facendo una ricerca per immagini su Google con la parola chiave "documento" la netta maggioranza dei risultati che ci si troverebbe davanti sarebbe costituita ancora da foto o icone di documenti cartacei... il documento moderno, e digitalmente rilevante, invece, non è più solo ciò che di primo acchito la nostra mente assocerebbe a questo nome, ovvero una "carta bollata", una lettera, un certificato, qualcosa che comunque possa esprimersi in una forma cartacea, ma qualcosa di molto più dinamico, strutturato e multicanale, come i flussi di informazioni che vengono scambiati e letti quotidianamente dai sistemi informativi e documentali sia delle PA che delle organizzazioni aziendali. Va da sé che nel gestire queste nuove tipologie di documenti si debbano mettere a punto sistemi multicanale e si debba tenere conto delle caratteristiche peculiari di questi flussi informativi, che, rispetto ai loro omologhi analogici, sono innanzitutto più facilmente modificabili e più difficilmente riconducibili al loro autore, viaggiano su canali tendenzialmente insicuri, sono sottoposti al continuo cambiamento tecnologico e, dulcis in fundo, non sono facilmente conservabili nel tempo.

⁶ *Documentare in digitale*, Editoriale di Andrea Lisi alla rivista Il Documento Digitale, Testata iscritta al tribunale di Roma n. 129/2012 del 3/5/2012. ISSN: 2280-4188, Trimestre gennaio-febbraio-marzo 2015, edita da LEX ET ARS.

⁷ Azioni di sensibilizzazione sono previste, ad esempio, nell'art. 8 del decreto legislativo n. 82/2005 (Codice dell'amministrazione digitale), il quale prevede in particolare che "lo Stato e i soggetti di cui all'articolo 2, comma 2, promuovono iniziative volte a favorire la diffusione della cultura digitale tra i cittadini con particolare riguardo ai minori e alle categorie a rischio di esclusione, anche al fine di favorire lo sviluppo di competenze di informatica giuridica e l'utilizzo dei servizi digitali delle pubbliche amministrazioni con azioni specifiche e concrete, avvalendosi di un insieme di mezzi diversi fra i quali il servizio radiotelevisivo".

⁸ Per una comprensione pratica delle diverse tipologie di firme elettroniche si consiglia la lettura del volume di Giovanni Manca *Le Firme elettroniche*, Edizioni Themis, 2021.

⁹ In ambito archivistico, il documento viene a coincidere con questa definizione: *Tutti i libri, le carte, le mappe, le fotografie o gli altri materiali documentari, indipendentemente dalla forma o dalle loro*

normative di documento informatico e documento elettronico andrebbero correttamente interpretate, cercando di favorire un approccio che ricomprenda anche una valutazione terminologica di base sui concetti di dato, informazione e documento, spesso utilizzati impropriamente dal legislatore, anche come sinonimi intercambiabili¹⁰.

Ormai si è passati da una concezione più tradizionale della formazione del documento prodotto attraverso un software di word processor o attraverso un'acquisizione della sua immagine via scanner a una visione più moderna e dinamica di documento, individuabile come una registrazione durevole di flussi informativi giuridicamente rilevanti.¹¹

Le varie tipologie di firma nel mondo digitale

Ma se il documento è cambiato radicalmente sviluppandosi attraverso piattaforme digitali, si avrà ancora in futuro la necessità di "firmare"? È una domanda a cui non è facile rispondere perché effettivamente si sta assistendo di recente a una serie di passaggi epocali che sottopongono continuamente la nostra esistenza a un incredibile mutamento comportamentale. Gestì, abitudini, anche modi di dire ci stanno cambiando radicalmente. Si scrive in modo diverso. Anzi, sempre più spesso, neppure si scrive, ma per comunicare si registrano in modo più o meno affidabile audio e video. Si fotografa in modo diverso, assumendo posizioni completamente differenti rispetto a quando

caratteristiche, prodotti o ricevuti da ogni pubblica o privata istituzione, nello svolgimento delle sue funzioni istituzionali o in connessione con la conduzione dei suoi affari particolari, e conservati, o degni di essere conservati, dalla stessa istituzione o dal suo successore, come testimonianza delle sue funzioni, della sua politica, delle decisioni, procedure, operazioni, o altre attività, o a causa del valore informativo dei dati ivi contenuti (Th.R.Schellenberg, *Modern Archives: Principles and Techniques*, Chicago, Illinois, Midway, 1975). Mentre in ambito diplomatico il documento può essere identificato con la *testimonianza scritta di un fatto di natura giuridica, compilata con l'osservanza di determinate forme, le quali sono destinate a procurarle fede e a darle forza di prova* (Cesare Paoli, *Diplomatica*, Firenze, Le Lettere, 1987, p.18).

Dal punto di vista strettamente giuridico non possono non ricordarsi le definizioni di *res signata* (Natalino Irti, 1969) o anche di *res rappresentativa di fatti giuridicamente rilevanti* (Francesco Carnelutti, *Teoria Moderna*, In *Novissimo Digesto Italiano*, 1975).

¹⁰ Tra le definizioni più rilevanti di documento a livello normativo si ricordano quelle di:

"documento informatico": documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti" (art. 1, comma 1, lett. p) nel Codice dell'amministrazione digitale contenuto nel Decreto legislativo 82/2005);

"documento analogico": documento non informatico (art. 1, comma 1, lett. p-bis Codice dell'amministrazione digitale);

"documento elettronico": qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva (Regolamento eIDAS - Regolamento (Ue) N. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che ha abrogato la direttiva 1999/93/CE);

"documento amministrativo": ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale (art. 22 L. 241/1990).

¹¹ La stessa locuzione latina *verba volant scripta manent* andrebbe riadattata e rimodellata in base ai nuovi strumenti di comunicazione multicanale di cui dispone oggi la società digitale e con essi deve fare i conti, ripensando allo stesso ruolo di terze parti fidate che possano cooperare con i contraenti/soggetti che manifestano le loro volontà in ambienti digitali riservando a tali manifestazioni di volontà espresse in modo diverso (sotto forma essenzialmente di file di log giuridicamente rilevanti) una staticizzazione e una conservazione in forma digitale autentica.

si affidavano i ricordi alla vecchia macchina a pellicola fotografica. E si documenta, quindi, in modo totalmente diverso la nostra memoria. E inevitabilmente si firma anche in modo diverso.

E garantire imputabilità giuridica, integrità, quindi, autenticità ai nuovi paradigmi della comunicazione dei nostri giorni sarà una difficile sfida. Gli stessi termini che si usano per determinare un futuro autentico alle nostre informazioni rilevanti e assegnarne così in modo affidabile l'appartenenza appaiono poco calzanti per il mondo digitale. Il termine documento, del resto, deriva dal latino docere (cioè, insegnare, rappresentare, dare prova) e, in senso più generico, è stato sempre considerato il documentum come un'informazione rilevante affissa in un supporto. E la stessa parola "sotto-scrizione" poco può adeguarsi alle caratteristiche del dato digitale. Ma se l'esigenza di appartenenza, di imputabilità giuridica in un mondo pervaso di bit (che hanno un significato giuridico o storico-archivistico) dovesse permanere, allora si dovranno necessariamente, da una parte cambiare i presupposti culturali, sociologici e quindi giuridici di questa appartenenza, e dall'altra trovare metodi affidabili per lasciare traccia, quindi memoria, alle nuove manifestazioni di volontà rappresentative di un'esistenza espressa in caratteri sempre più digitali. Quindi, non potrà essere più l'affidabilità di un supporto a dover resistere nel tempo, perché il cuore pulsante dei bit può e deve essere garantito in modo diverso e certificabile, prescindendo dal fardello del supporto che ha dovuto faticosamente preservare negli anni le rappresentazioni del nostro tempo.

Sono domande ed esigenze quelle che ci si pone che si intersecano tra loro rivestendo un'importanza strategica nell'evoluzione del pensiero giuridico e con esse ci si continuerà a confrontare nell'immediato futuro, laddove si vorrà/dovrà fare i conti con le delicate esigenze della custodia affidabile di nostri dati, informazioni e documenti.

La validità formale e probatoria del documento informatico

La validità e l'efficacia probatoria del documento informatico sono disciplinate nell'ordinamento italiano dall'art. 20 del Codice dell'amministrazione digitale (di seguito CAD), in base al quale un documento informatico soddisfa il requisito della forma scritta (acquisendo anche il valore probatorio di cui all'art. 2702 Cod. civ., ossia della scrittura privata) quando vi sia apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, quando esso sia formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID¹² con modalità tali da garantire sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore¹³.

¹² Si fa riferimento all'Agenzia per l'Italia Digitale - <https://www.agid.gov.it/>.

¹³ Art. 20, comma 1-bis, CAD: "Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile 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'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili

La formulazione dell'art. 20 del CAD, dunque, ricomprende il documento informatico che abbia le caratteristiche e rispecchi determinati requisiti (sicurezza, integrità e immodificabilità) e a cui sia apposta una qualunque firma elettronica, anche una firma elettronica semplice (purché, appunto, la riconducibilità all'autore sia "manifesta e inequivoca"). Le disposizioni dell'art. 20 del CAD risultano, quindi, in linea con l'attuale concezione di documento informatico prevista nel CAD e con quella di documento elettronico, prevista dal Regolamento eIDAS (Reg. 910/2014/UE). In tal senso, documento informatico è il "contenuto" che si dovrebbe adattare a molti "contenitori" per essere formato, gestito e conservato, e che può avere, infatti, molti formati, molte firme, può essere oggetto di molti strumenti di trasmissione, purché ne siano sempre preservate la sicurezza, l'immodificabilità e l'integrità¹⁴. Nello specifico, dunque, il documento non deve essere necessariamente scritto o redatto sotto forma di un testo, bensì può essere costituito da un qualsiasi flusso di dati in forma elettronica: l'importante è che tale contenuto sia "stored", cioè reso statico e preservato nella sua integrità nel tempo.

L'evoluzione della sottoscrizione nel mondo digitale

Inoltre, se prima i documenti dovevano essere necessariamente firmati e sottoscritti¹⁵, ora i documenti informatici sono formati e trasmessi attraverso partner fidati; non a caso, infatti, il Regolamento eIDAS si occupa di identificazione elettronica e servizi fiduciari. Il partner fidato, che garantisce certi processi informatici o eroga "servizi fiduciari"¹⁶, è il soggetto che – previa verifica di affidabilità da parte delle autorità competenti nel caso in cui siano soggetti "qualificati"¹⁷ – concorre alla formazione, gestione, firma, trasmissione e conservazione dei documenti informatici¹⁸.

Viene sancita, dunque, un'ulteriore evoluzione, anzi un vero e proprio passaggio epocale: dal "segnare" un documento al "consegnare" un documento (informatico). Proprio in questa prospettiva, in effetti, le firme elettroniche "non firmano" (o meglio non sottoscrivono), ossia non sono apposte "sul documento" per attribuirne l'imputabilità giuridica, bensì sono associate a quel contenuto giuridicamente rilevante, "validando" processi digitali: esse, cioè, attribuiscono quel contenuto – con

in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida"

¹⁴ Secondo la definizione di cui al Glossario dei termini e degli acronimi, Allegato 1 alle "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" di AgID, per "integrità" si intende la caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.

¹⁵ Rimane di attualità quanto scrivevo in proposito su Altalex in data 16/03/2004 sull'evoluzione della sottoscrizione autografa nei rapporti "privatistici" telematici reperibile qui <https://www.altalex.com/documents/news/2004/03/16/evoluzione-della-sottoscrizione-autografa-nei-rapporti-privatistici-telematici>.

¹⁶ Art. 4 Regolamento eIDAS 910/2014 UE.

¹⁷ Si veda la definizione di prestatori di servizi fiduciari qualificati di cui all'art. 4 Reg. eIDAS.

¹⁸ Questo vale almeno per quanto riguarda genericamente il nostro attuale sistema giuridico nazionale. Nel regolamento eIDAS, come sappiamo, la conservazione, come servizio qualificato, è previsto solo in relazione a firme e sigilli elettronici qualificati. Tematica questa che meriterebbe comunque uno specifico approfondimento, anche in relazione alle ultime novità che riguardano i conservatori accreditati e che – ai fini della presente pubblicazione – mi limito a ricordare, rinviando ad altre più specifiche pubblicazioni sul punto.

un diverso valore giuridico e probatorio in base alla sicurezza e all'affidabilità del processo – a un determinato soggetto dell'ordinamento. Costituisce un esempio concreto in Italia di tali processi la cosiddetta "firma SPID¹⁹". Tale nuova tipologia di firma²⁰, infatti, seppur non espressamente menzionata, è ovviamente ricompresa nel novero delle firme elettroniche dall'art. 20 del CAD²¹.

Firme elettroniche e articolo 20 CAD

L'art. 20 del CAD, come già in precedenza sinteticamente rilevato, non disciplina esclusivamente il valore giuridico e probatorio dei documenti a cui siano associate firme digitali²², firme elettroniche qualificate o firme elettroniche avanzate, bensì qualsiasi firma elettronica, anche le firme elettroniche c.d. semplici (ad es. le e-mail o le transazioni e-commerce), che quindi possono essere idonee ad attribuire il valore di forma scritta al documento informatico a cui sono associate, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità, valutabili discrezionalmente da un giudice.

Tuttavia, l'art. 20 del CAD stabilisce che per attribuire al documento informatico il valore giuridico di forma scritta non sia sufficiente solo garantire la sua riconducibilità all'autore²³ (attraverso una firma elettronica), ma è necessario che sia formato attraverso un processo avente i requisiti fissati dall'AgID, ai sensi dell'articolo 71, ossia attualmente con le Linee guida sulla formazione, gestione e conservazione dei documenti informatici²⁴.

¹⁹ Per SPID si intende ovviamente il Sistema Pubblico di Identità Digitale.

²⁰ Si veda in argomento la Determinazione AgID n.157/2020, con la quale sono state emanate le Regole Tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD.

²¹ Trattasi di firma che non trova invece una sua tipizzazione nel Regolamento eIDAS.

²² In argomento si ricorda che "l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria" (art. 20, co. 1-ter, CAD) e che "salvo il caso di sottoscrizione autenticata, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile redatti su documento informatico o formati attraverso procedimenti informatici sono sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale ovvero sono formati con le ulteriori modalità di cui all'articolo 20, comma 1-bis, primo periodo." (art. 21, co. 2-bis, CAD, rubricato "Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale").

²³ Forse sarebbe più corretto riferirsi al soggetto a cui attribuire l'imputabilità giuridica del documento, in modo che non possa confondersi in via interpretativa con il soggetto che "materialmente" forma il documento.

²⁴ Linee guida già in vigore e che dal gennaio 2022 sostituiranno:

- il DPCM 13 novembre 2014, contenente "Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici";
- il DPCM 3 dicembre 2013, contenente "Regole tecniche in materia di sistema di conservazione".
- Per quanto concerne il DPCM 3 dicembre 2013, contenente "Regole tecniche per il protocollo informatico", sono abrogate tutte le disposizioni, ad eccezione di alcune.

Per un'analisi puntuale delle Linee guida si rinvia a *Conservazione dei documenti, ecco tutte le regole nelle linee guida Agid* di Luigi Foglia e Andrea Lisi pubblicato su AgendaDigitale.eu disponibile alla pagina <https://www.agendadigitale.eu/documenti/conservazione-dei-documenti-ecco-tutte-le-regole-nelle-linee-guida-agid/>. Per una breve analisi delle ultime modifiche intervenute sulle Linee Guida si consiglia la lettura di *Linee Guida AgID sul documento informatico modificate e rinviate al 1° gennaio 2022* di Mario Montano pubblicato su Anorc.eu alla pagina <https://anorc.eu/attivita/linee-guida-agid-sul-documento-informatico-modificate-e-rinviate-al-1-gennaio-2022/>.

Per analizzare alcune criticità della recente regolamentazione AgID si consiglia la lettura di *Conservazione, perché il regolamento Agid distrugge il mercato* di Luigi Foglia e Andrea Lisi pubblicato su AgendaDigitale.eu

Sulla scorta dell'art. 20 del CAD, dunque, per attribuire il valore giuridico di forma scritta a un documento informatico, quest'ultimo deve comunque essere "formato attraverso un processo" che sia conforme a quanto stabilito dalle Linee guida AgID. Tali Linee guida prevedono – tra gli altri requisiti – che al momento della formazione del documento informatico imm modificabile, siano generati e associati permanentemente ad esso i relativi metadati²⁵. Presupposto essenziale di validità di documenti informatici e firme rimane pertanto la loro corretta e affidabile custodia in modo autentico che ne preservi nel tempo l'affidabilità giuridica, quindi, garantisca a dati e metadati giuridicamente rilevanti sicurezza, integrità e imm modificabilità e, in maniera manifesta e inequivoca, la loro riconducibilità all'autore.

La conservazione dei documenti informatici non si fa in cloud o in blockchain

La materia della custodia di contenuti digitali è complessa e delicata e andrebbe affrontata, quindi, con particolare attenzione sistematica. Purtroppo, si leggono in questi giorni molti slanci interpretativi sull'argomento della formazione, gestione e conservazione dei documenti informatici che arrivano a proporre soluzioni miracolose in cloud, o peggio, in blockchain. Alcune di esse potrebbero apparire persino esilaranti nella loro surrealtà (e purtroppo un certo semplicismo di approccio al cloud si respira anche nelle ultime Linee Guida AgID²⁶), ma il rischio è che – considerata la problematicità dell'argomento – possano essere prese in considerazione con una certa serietà a causa del dilagante pressapochismo che sembra caratterizzare purtroppo chi "si occupa di digitale" oggi in Italia. Credo che sia giusto ricordare invece che – come già in parte anticipato - per garantire il mantenimento in ambiente digitale della memoria autentica di dati, informazioni e documenti gestiti in un contesto archivistico, il nostro Paese si è attrezzato per tempo con una normativa tecnica che ha le sue radici su principi generali contenuti nella legislazione primaria (nel CAD, cioè nel più volte citato Codice dell'amministrazione digitale). E si può anche riferire, senza paura di essere smentiti, che da anni siamo all'avanguardia in questo specifico e delicato settore, ma ultimamente sembra quasi che si debba vergognarsi di questa particolare expertise maturata nel tempo, perché occorre in qualche modo far confluire tutti questi argomenti verso le nuove mode tecnologiche del momento.

Questo atteggiamento è evidentemente pericolosissimo.

Dovrebbe invece essere chiaro ormai che la memoria digitale, secondo la normativa primaria e tecnica che si è evoluta in tutti questi anni, viene assicurata non da un singolo strumento software, non da un applicativo o da una singola soluzione, ma da un sistema complesso che parte dalla formazione

disponibile alla pagina <https://www.agendadigitale.eu/documenti/conservazione-perche-il-regolamento-agid-distrugge-il-mercato/>.

²⁵ Si veda par. 2.1.1 delle Linee guida dedicato alla formazione del documento informatico. L'insieme dei metadati del documento informatico, in particolare, è definito nell'allegato 5 "Metadati" alle Linee guida.

²⁶ Una lettura critica alle Linee guida AgID si respira in molte prese di posizione dell'associazione ANORC (Associazione Nazionale Operatori e Responsabili della Custodia di contenuti digitali – www.anorc.eu). Info utili sulle critiche espresse sono reperibile a questo link: <https://www.dire.it/27-07-2021/657472-digitale-anorc-servono-regole-chiare-per-la-conservazione-dei-documenti/>.

coerente dei documenti informatici ed è in grado di preservare il loro legame (meglio noto come vincolo) archivistico per tutto il tempo di conservazione previsto ex lege.

L' ABC della "digitalizzazione"

È utile allora fare sintetica chiarezza su principi basilari che chiunque intenda accostarsi all'abusato termine "digitalizzazione" dovrebbe conoscere a memoria, prima di scrivere - o peggio di guidare le scelte strategiche di un Paese - su questi argomenti. Prima di tutto, ci si sta occupando di un argomento di una incredibile rilevanza, pur se spesso ignorato: il mantenimento della memoria autentica di documenti e fascicoli in ambiente digitale. In poche parole, ci si sta interessando dello sviluppo in ambiente digitale degli archivi, dai quali – come si dovrebbe sapere – dipende la nostra stessa democrazia²⁷.

Per garantire l'autenticità di un documento occorre preservarne non solo la sua integrità e leggibilità nel tempo, ma anche assicurarne il contesto archivistico. Sembra che si stia banalizzando molto invece il concetto di mantenimento della memoria in un contesto ormai dinamico, quello digitale (o peggio "social"), dove la certezza delle fonti è messa costantemente a dura prova e non si può rischiare di confondere la conservazione di un archivio con un semplice backup assicurato a basso costo da un cloud provider. Risulta opportuno procedere allora con un minimo di ordine su argomenti di grande rilievo per il futuro della nostra memoria digitalmente autentica.

La moda passa. La memoria digitale resta.

Secondo quanto previsto nell'articolo 43 del CAD, "gli obblighi di conservazione e di esibizione di documenti si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le relative procedure sono effettuate in modo tale da garantire la conformità ai documenti originali e sono conformi alle Linee guida²⁸" e, ancora più nello specifico, nello stesso articolo viene precisato che " i documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle Linee guida". Ciò che non è chiaro ai più è che secondo la legislazione italiana (e in realtà secondo qualsiasi logica giuridico-archivistica, oltre che informatica) per conservare documenti e fascicoli in formato digitale occorre predisporre un sistema dinamico, complesso e organizzato in termini di risorse umane e tecnologiche, in grado di rispettare

²⁷ "Archivi pubblici come baluardo della democrazia". A sostenere questo parallelismo è stato Barack Obama nel suo discorso di insediamento alla Casa Bianca, il 20 gennaio 2009. Una volta erano polverose pergamene, poi pesanti libroni cartacei rilegati in cuoio. Ora solo bit. Ma non c'è dubbio che la fede pubblica di certificati di proprietà, stati di famiglia, atti di nascita dipende da una loro corretta digitalizzazione... Così Marino Longoni su ITALIAOGGI SETTE - numero 186 06/08/2012 acquisibile alla pagina <https://www.italiaoggi.it/archivio/dati-pubblici-alla-deriva-1783956>.

²⁸ Fino al gennaio 2022 coesisteranno le Regole Tecniche contenute nel DPCM 3 dicembre 2013 e le più volte citate Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

precisi standard, anche di carattere internazionale ...e non semplicemente affidarsi all'app o alla tecnologia più di moda del momento.

Infatti, l'art. 44 del CAD definisce i requisiti dei sistemi di gestione e conservazione dei documenti e dei fascicoli informatici, definendo ruoli e responsabilità per assicurare il mantenimento della memoria autentica nel tempo. In particolare, il sistema di conservazione dei documenti informatici deve assicurare, per quanto in esso conservato, caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità, secondo le modalità indicate nelle normative tecniche. Le attuali regole contenute nelle Linee guida AgID, in attuazione di quanto previsto dal Codice nell'art. 44, definiscono i requisiti tecnici e organizzativi che i vari responsabili dei sistemi di gestione e di conservazione documentale devono assicurare, coordinandosi in un vero e proprio team di carattere interdisciplinare a disposizione delle organizzazioni pubbliche o private, che ha come compito quello di tutelare il mantenimento della pubblica fede degli archivi digitali.

Le strade praticabili (quelle vere)

Quindi, ciò che si deve sviluppare per assicurare il mantenimento della memoria digitale nel tempo non è un applicativo che segua certi standard o la predisposizione di una semplice e banale procedura che assicuri uno stabile back up e un disaster recovery a dati informatici, ma occorre mettere in atto e organizzare diversi team di responsabili con professionalità diverse che tra loro collaborino per sviluppare, mantenere e controllare sistemi complessi (di formazione, gestione e conservazione) di documenti e fascicoli informatici. Questa - e solo questa - è la conservazione (che va intesa come sistema), che può essere sviluppata internamente da organizzazioni pubbliche e private o essere affidata all'esterno ad outsourcee preparati e affidabili (i cosiddetti conservatori di documenti informatici). Le pubbliche amministrazioni in particolare, ex art. 34 del CAD, possono procedere alla conservazione di documenti informatici o sviluppandola all'interno della propria struttura organizzativa oppure affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati (che possono qualificarsi come conservatori presso l'AgID)²⁹.

Questi soggetti esterni quindi – lo si ripete – devono sviluppare non una semplice soluzione software da mettere a disposizione di una PA (o di un'impresa), ma devono garantire la predisposizione di un sistema complesso di conservazione in termini di risorse umane, tecnologiche e organizzative in grado di garantire tutto ciò che le normative primaria e secondaria prevedono e naturalmente essere *compliant* con gli standard (normative tecniche ISO ed ETSI) da esse richiamati.

²⁹ Le pubbliche amministrazioni possono procedere alla conservazione dei documenti informatici:

a) all'interno della propria struttura organizzativa;

b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle Linee guida di cui all'art. 71 relative alla formazione, gestione e conservazione dei documenti informatici nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione.

Così comma 1bis art. 34 del Codice dell'amministrazione digitale.

La Blockchain: fuori una

Sulla base di questi presupposti, quindi, è ridicolo anche solo pensare di poter offrire la conservazione in blockchain. È proprio sbagliato concettualmente il punto di partenza di tale affermazione³⁰.

Al massimo, ci si può interrogare su come una soluzione basata su registri distribuiti possa tecnologicamente garantire alcune specifiche esigenze (nella corretta formazione del documento) che i sistemi di gestione e conservazione devono poi assicurare. Questo è il termine giusto con cui ci si può rapportare a uno strumento tecnologico nuovo e che può – come qualsiasi strumento utile a garantire integrità e staticità a dati di natura digitale – essere verificato di volta nella sua specifica ed eventuale efficacia, appunto, nelle fasi dinamiche di formazione di un documento informatico.

Il Cloud: il (dis)orientamento della PA

Altra precisazione va fatta sul cloud, soprattutto nel mondo delle PA dove la confusione è imperante. Come si sa – o si dovrebbe sapere – ex art. 68 del CAD le pubbliche amministrazioni devono acquisire programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:

- a) software sviluppato per conto della pubblica amministrazione;
- b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;
- c) software libero o a codice sorgente aperto;
- d) software fruibile in modalità cloud computing;
- e) software di tipo proprietario mediante ricorso a licenza d'uso;
- f) software combinazione delle precedenti soluzioni.

Il cloud (nelle sue differenti accezioni IaaS, PaaS o SaaS), quindi, ex lege va considerato come una soluzione informatica offerta “a catalogo” in modalità cloud, e non può di certo assumere le connotazioni di un sistema complesso di gestione documentale e conservazione³¹. Ma non si può

³⁰ La tecnologia blockchain non è utile a garantire la custodia dei documenti informatici al pari di un sistema di conservazione documentale, ma semplicemente potrebbe garantirne l'integrità tramite il versamento nei registri distribuiti delle impronte degli stessi.

Una profonda critica alla moda della tecnologia blockchain è arrivata da Andrea Monti su Italian.Tech alla pagina https://www.italian.tech/blog/strategikon/2021/07/20/news/blockchain_criptovalute_nft_e_smart_contra_cks_l_illusione_della_liberta_-310844639/.

³¹ A livello di Sistema Paese, accanto ai Poli Strategici Nazionali (PNS) c'è una precisa strategia nazionale sul Cloud della PA che è nata nei suoi intenti programmatici per favorire l'adozione del modello del cloud computing nelle pubbliche amministrazioni italiane, in linea con le indicazioni della Strategia per la Crescita

confondere ancora oggi il cloud provider qualificato con il conservatore³². Sono soggetti distinti, che offrono attività completamente diverse. Un cloud provider qualificato può offrire quindi un qualsiasi servizio in modalità cloud SaaS, PaaS e IaaS, mentre il conservatore (a maggior ragione quando è qualificato) è in grado di sviluppare un complesso sistema basato su risorse umane, organizzative e tecniche, che di fatto sostituisce in tutto o in parte il sistema archivistico di conservazione dell'ente pubblico. Non si possono confondere concetti così elementari dal punto di vista tecnico-giuridico, almeno per chi conosce la materia da tanto tempo, e non ci si può permettere ancora di "navigare a vista" su certi concetti fondamentali.

Ovvio, quindi, che una PA potrà decidere di sviluppare in house (quindi internamente) il proprio sistema di conservazione e utilizzare così per lo sviluppo di tale sistema un applicativo che ex art. 68 CAD potrà essere offerto da un fornitore con licenza proprietaria, open source o fruibile "in modalità cloud" e, in quest'ultimo caso, il cloud provider dovrà essere necessariamente qualificato da AgID. Oppure la stessa PA potrà decidere di affidare in outsourcing (quindi all'esterno) il proprio sistema di conservazione a un conservatore che dovrà osservare scrupolosamente le normative secondarie portate avanti da AgID, ma questo complesso affidamento in outsourcing non è e non può ritenersi una "modalità cloud" di conservazione dei documenti informatici.

Va evitata confusione su questi aspetti, anzi sarebbe auspicabile un impegno collettivo (da parte di decisori pubblici, mercato e professionisti del settore) perché sia sempre garantito un percorso davvero serio, rigoroso e affidabile per i nostri documenti informatici che parta dalla loro formazione (a prescindere dai tanti applicativi o soluzioni utilizzabili per assicurarne l'integrità e immodificabilità), ne garantisca una corretta fascicolazione (in un sistema affidabile di gestione) fino a garantirne la memoria autentica nel tempo, preservandone il contesto archivistico (attraverso un rigoroso sistema di conservazione).

La bacchetta magica del cloud o della tecnologia blockchain almeno in questo caso lasciamola ai prestigiatore.

Conclusioni

Per poter, quindi, gestire correttamente queste nuove tipologie di documenti e informazioni rilevanti occorre necessariamente adottare specifici modelli e metodologie "a norma", finalizzati a garantire l'attribuibilità, l'integrità, l'autenticità, la sicurezza, la corretta archiviazione e la conservazione nel tempo al patrimonio intangibile di dati digitali.

digitale del Paese e con le previsioni del Piano Triennale per l'Informatica nella Pubblica Amministrazione 2019 – 2021.

Tale strategia delineata da AgID prevede un percorso di qualificazione per i soggetti pubblici e privati che intendono fornire infrastrutture e servizi cloud alla pubblica amministrazione, affinché queste ultime possano adottare servizi e infrastrutture di cloud computing omogenei, che rispettino elevati standard di sicurezza, efficienza ed affidabilità, in linea con le previsioni delle circolari AgID n.2 e n. 3 del 9 aprile 2018.

³² Sui complessi rapporti tra conservazione e cloud è intervenuto Luigi Foglia su AgendaDigitale.eu in *Conservazione accreditata Agid in cloud? Ma le norme vanno rifatte, ecco perché* acquisibile alla pagina <https://www.agendadigitale.eu/documenti/conservazione-accreditata-agid-in-cloud-ma-le-norme-vanno-rifatte-ecco-perche/>.

Sotto un certo punto di vista si potrebbe affermare che la dinamicità e l'inafferrabilità di queste informazioni digitali siano paragonabili a quelle della parola, della volontà espressa oralmente. Oggi, per comprendere la realtà digitale e le sue dinamiche evolutive (anche dal punto di vista giuridico), è utile probabilmente riflettere sul fatto che per garantire ufficialità e valore giuridico alla volontà orale ci si è serviti per secoli, e tuttora ci si serve, dell'intervento di un pubblico ufficiale, di un notaio che, prestato orecchio ai desideri del cliente o dei soggetti che manifestano in sua presenza la loro volontà in forma collegiale, li trasforma in un documento inoppugnabile (cartaceo o digitale che sia); allo stesso modo, per stabilizzare e preservare nel tempo il valore giuridico di questi flussi di informazioni digitali che ormai costituiscono la forma più evoluta e affascinante delle rappresentazioni informatiche di fatti, atti, dati giuridicamente rilevanti, è necessario che ci sia l'intervento di una terza parte fidata: il Responsabile della conservazione digitale. Il Responsabile della conservazione digitale dei documenti potrebbe essere definito oggi come "il custode dell'autenticità del documento privo di peso" e sua è la grande responsabilità di dominare in un'organizzazione pubblica o privata tutti i flussi di informazioni e documenti che l'attraversano – sia che provengano dall'interno che dall'esterno – e gestirli in ogni fase, dalla creazione alla conservazione, garantendo, attraverso avanzate tecniche di conservazione digitale, a tutti i dati che abbiano un rilievo giuridico la certa paternità, la corretta trasmissibilità e gestione, l'adeguata fascicolazione e archiviazione e, non da ultimo, la necessaria sopravvivenza nel tempo. Un ruolo cruciale quello del Responsabile conservazione, che richiede, quindi, una preparazione accurata, mirata e multidisciplinare.

Tale figura si interseca con quella del Responsabile della protezione dei dati personali e insieme possono coordinare e guidare, all'interno di team necessariamente interdisciplinari, progetti di trasformazione digitale che aspirino a garantire l'autenticità e l'affidabilità a tutto il patrimonio documentale, di enti pubblici e privati: una profonda trasformazione che ormai ha riversato le sue radici lungo la "leggerezza dei bit".

Sitografia

<https://www.agid.gov.it/>

<https://anorc.eu/>

<http://www.interpares.org/>

<https://www.procedamus.it/>

Bibliografia essenziale

Conti G. "Lineamenti di diritto delle piattaforme digitali", Maggioli editore, vol. 1 e 2, 2020-2021;

Foglia L., Conservazione accreditata Agid in cloud? Ma le norme vanno rifatte, ecco perché, AgendaDigitale.eu, 2019;

Foglia L., A. Lisi, Conservazione dei documenti, ecco tutte le regole nelle linee guida Agid, AgendaDigitale.eu, 2020;

Limone D. , Burocrazie agili: prototipi di amministrazioni semplificate e digitali. Come procedere?, Key4biz, 2020;

Lisi A. (a cura di) Conservazione dei documenti informatici. Aspetti giuridici, fiscali, amministrativi e strategici della conservazione sostitutiva e della fatturazione elettronica, Roma, Edizioni CieRre S.r.l., 2007;

Lisi A., Evoluzione della sottoscrizione autografa nei rapporti "privatistici" telematici, Altalex, 2004;

Manca G., Le Firme elettroniche, Edizioni Themis, 2021;

Pascuzzi G, il diritto nell'era digitale, il Mulino. 2020

Penzo Doria G. La conservazione del documento digitale, Interlex, 2006.



Associazione Nazionale per Operatori e Responsabili della Custodia
dei dati, delle informazioni e dei documenti digitali

Documento associativo

Ottobre 2021

Segreteria

segreteria@anorc.it
+39 0832 256065

Direzione

direzione@anorc.it

Ufficio Comunicazione

comunicazione@anorc.it

