Il valore giuridico e probatorio delle firme elettroniche tra neutralità tecnologica, non discriminazione e certezza del diritto*

Fernanda Faini

Abstract

Il contributo intende analizzare la disciplina normativa europea e nazionale in materia di documenti informatici e firme elettroniche. In particolare, il saggio esamina il diverso valore giuridico e probatorio dei documenti informatici in relazione alle differenti tipologie di firma elettronica che caratterizzano l'ordinamento, anche alla luce dei principi che governano la materia, quali neutralità tecnologica e non discriminazione. L'analisi è tesa ad affrontare gli aspetti critici che scaturiscono dall'applicazione concreta delle disposizioni a strumenti specifici e tecnologie determinate, sviluppando alcune riflessioni al riguardo.

The contribution aims to analyze the European and national legal framework concerning electronic documents and electronic signatures. In particular, the paper examines the different legal and evidentiary value of electronic documents in relation to the different types of electronic signatures that characterize the legal system, also in the light of the principles that govern the matter, such as technological neutrality and non-discrimination. The analysis deals with the critical aspects that arise from the concrete application of the provisions to specific tools and technologies, developing some reflections in this regard.

Sommario

* Il saggio è stato realizzato nell'ambito delle attività del Progetto PRIN 2017 "*Self- and Co-regulation for Emerging Technologies: Towards a Technological Rule of Law*".
L'articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio "a doppio cieco".

Keywords

documento informatico – firme elettroniche – firma digitale – regolamento (UE) n. 910/2014 – d.lgs. 82/2005

1. L'impatto delle tecnologie informatiche sugli strumenti giuridici

L'evoluzione tecnologica, che ha reso centrale la dimensione digitale nell'esistenza umana, impatta in modo determinante sui documenti e sugli atti del mondo privato e pubblico; secondo l'immagine evocativa di Renato Borruso, gli elettroni sono il nuovo inchiostro, i bit il nuovo alfabeto e le memorie del computer la nuova carta[1].

Le tecnologie dell'informazione e della comunicazione incidono profondamente sulla vita degli individui e delle istituzioni, portati ad avvalersi con frequenza crescente dei nuovi strumenti digitali, in considerazione dei vantaggi che permettono di realizzare. Le nuove tecnologie, infatti, consentono di superare gli ostacoli costituiti dalle barriere del tempo e dello spazio, dal momento che rendono le comunicazioni e i rapporti semplici e immediati, prescindendo dalle distanze geografiche e dalla necessaria presenza fisica. Queste caratteristiche, unite all'economicità e all'efficacia degli strumenti digitali e potenziate dalla possibilità di accesso alla rete tramite diversi *device*, anche mobili, hanno portato alla digitalizzazione di attività private e pubbliche, le cui rappresentazioni informatiche acquisiscono valore giuridico e producono effetti nell'ordinamento. Gli individui compiono numerose azioni nella dimensione digitale, incontrano opportunità, intrecciano relazioni e concludono negozi giuridici.

Il nuovo volto digitale della società disvela però anche problematiche giuridiche inedite e nuove esigenze di sicurezza. Nel regolare l'innovazione, infatti, il diritto è chiamato a garantire adeguata certezza ai rapporti tra soggetti e, a tal fine, ad assicurare validità ai documenti formati e trasmessi e alle attività giuridiche compiute per mezzo delle tecnologie informatiche, in modo che gli strumenti digitali possano offrire le stesse garanzie in termini di affidabilità degli strumenti analogici.

L'ordinamento giuridico, al fine di attribuire rilevanza a fatti e attività, ha necessità di rappresentarli attraverso il documento e di rendere tale rappresentazione stabile e immutabile nel tempo e nello spazio, al fine di conferire certezza alle relazioni giuridiche. Per tali ragioni l'ordinamento si preoccupa della forma degli atti giuridici e prevede regole atte a disciplinare l'attività documentale[2].

Pertanto, come il documento cartaceo nel mondo analogico, parimenti il documento informatico costituisce oggetto privilegiato delle attività giuridiche digitali; di conseguenza, è centrale la relativa disciplina normativa.

[1] R. Borruso, *Computer e diritto*, tomo II, Milano, 1988, 218 ss.

[2] Cfr. G. Pascuzzi (a cura di), *Il diritto dell'era digitale*, V ed., Bologna, 2020, 113 ss.

Al riguardo rilevano le caratteristiche stesse della dimensione digitale, in particolare l'identità digitale dei soggetti, l'intangibilità degli oggetti e i mutamenti nelle dimensioni di tempo e spazio, determinate dall'impatto delle tecnologie informatiche; il superamento dei confini territoriali genera l'esigenza di omogeneità nelle risposte giuridiche degli ordinamenti, motivo del ruolo significativo assunto dalla normativa sovranazionale in materia.

La normativa si è preoccupata di dettare disposizioni idonee ad assicurare la certezza del diritto grazie alla previsione di disposizioni atte a preservare, nel caso dei documenti informatici, gli aspetti necessari e caratterizzanti del documento *in re ipsa*, quali, in particolare, l'oggetto costituito dal documento, ossia in particolare l'autenticità, l'integrità e l'immodificabilità del documento stesso (l'aspetto oggettivo, il "cosa"), l'identificazione del soggetto giuridico cui imputare la paternità del documento informatico (l'aspetto soggettivo, il "chi") e l'individuazione temporale (l'aspetto temporale, il "quando").

Le norme e le regole tecniche, infatti, disciplinano le caratteristiche necessarie a garantire l'autenticità, l'integrità e l'immodificabilità del documento (l'aspetto oggettivo), le firme elettroniche (l'aspetto soggettivo) e i riferimenti temporali atti a dimostrare l'esistenza di un'evidenza informatica in un tempo certo (l'aspetto temporale)[3].

Il contributo intende analizzare la disciplina normativa europea e nazionale in materia di documenti informatici e firme elettroniche. In particolare, il lavoro esamina il diverso valore giuridico e probatorio dei documenti informatici in relazione alle differenti tipologie di firma che caratterizzano l'ordinamento, anche alla luce dei principi che governano la materia, quali neutralità e non discriminazione. L'analisi è tesa ad affrontare gli aspetti critici che scaturiscono dall'applicazione concreta delle disposizioni a tecnologie e strumenti specifici, delineando alcune direzioni future.

2. Il *framework* giuridico europeo e nazionale

Le disposizioni normative principali relative al documento informatico e alle firme elettroniche a livello europeo sono contenute nel regolamento (UE) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (*electronic IDentification Authentication and Signature*, cosiddetto regolamento eIDAS)[4].

Alla luce delle esigenze di omogeneità che scaturiscono dall'abbattimento dei confini geografici nella dimensione digitale, significativamente il legislatore europeo ha scelto in materia lo strumento giuridico del regolamento e non della direttiva: il regolamento eIDAS si pone quale strumento di uniformazione che mira a realizzare l'interoperabilità giuridica e tecnica fra i Paesi europei degli strumenti elettronici di identificazione, autenticazione e firma, al fine di rafforzare la fiducia nelle transazioni elettroniche nel

[3] Reg. (UE) n. 910/2014, d.lgs. 82/2005 (art. 20 ss.) e relative regole tecniche.

[4] Il reg. (UE) n. 910/2014 (di seguito anche regolamento eIDAS) abroga la direttiva 1999/93/CE e si applica pienamente per la maggioranza delle sue disposizioni dal 1° luglio 2016.

mercato interno e garantire il reciproco riconoscimento dell'identificazione elettronica, dell'autenticazione, delle firme e di altri servizi fiduciari oltre confine, aumentando così l'efficacia dei servizi online pubblici e privati nell'Unione europea[5]. Il regolamento europeo ha ampiamente attinto alla legislazione nazionale in materia, già particolarmente sviluppata, dal momento che l'ordinamento italiano è stato uno dei primi a dotarsi di una disciplina organica circa il pieno riconoscimento della validità giuridica della firma digitale.

A livello nazionale la normativa in materia di documento informatico e firma digitale, prima contenuta nella legge 59/1997 e nel relativo d.p.r. 513/1997, che hanno riconosciuto validità ad atti e contratti formati da privati e pubbliche amministrazioni mediante strumenti informatici e trasmessi in via telematica, prevedendo una clausola di equivalenza tra sottoscrizione autografa e firma digitale, è confluita in un primo momento nel d.p.r. 445/2000 e, dopo l'intervento del d.lgs. 10/2002 e del relativo d.p.r. 137/2003, che hanno recepito la direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche, ha trovato collocazione nel d.lgs. 82/2005.

Pertanto le disposizioni atte a regolare documenti informatici e firme elettroniche sono contenute oggi prevalentemente, seppur non esaustivamente, nel Codice dell'amministrazione digitale (CAD), il d.lgs. 82/2005, come scaturente dalle modifiche e integrazioni anche recenti (quali il d.lgs. 179/2016, il d.lgs. 217/2017 e, da ultimo, il d.l. 76/2020, convertito con modificazioni dalla legge 120/2020)[6], nella normativa secondaria e nelle linee guida recanti le regole tecniche[7]. In merito le linee guida sulla formazione, gestione e conservazione dei documenti informatici sono state pubblicate il 10 settembre 2020, data dell'entrata in vigore, e sono state oggetto di modifiche e integrazioni il 18 maggio 2021; l'applicazione e l'attuazione delle stesse è stata prevista entro il 1° gennaio 2022[8].

In materia, infatti, i principi giuridici recati dalle norme si realizzano nelle regole di

[5] In considerazione della natura dello strumento giuridico utilizzato, ossia regolamento europeo e non direttiva, si tratta di un mezzo di uniformazione e non di armonizzazione; cfr. G. Finocchiaro, *Una prima lettura del Reg. UE n. 910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari*, in *Le nuove leggi civili commentate*, 3, 2015, 422 ss.

[6] Il d.lgs. 82/2005 è stato modificato in particolare sotto tali profili dai d.lgs. 159/2006, d.lgs. 235/2010, d.l. 179/2012, convertito con modificazioni dalla legge 221/2012, d.lgs. 179/2016, d.lgs. 217/2017 e d.l. 76/2020, convertito con modificazioni dalla legge 120/2020; da tenere in considerazione al riguardo, altresì, il d.lgs. 10/2010, in materia di atto pubblico informatico redatto dal notaio. Cfr. G. Finocchiaro, *Firme elettroniche e firma digitale*, in G. Finocchiaro – F. Delfini (a cura di), *Diritto dell'informatica*, Torino, 2014, 309 ss.; A.C. Amato Mangiameli, *Informatica giuridica. Appunti e materiali ad uso di lezioni*, II ed., Torino, 2015, 257 ss.

[7] Le regole tecniche sono approvate con linee guida, ai sensi degli artt. 20 e 71, d.lgs. 82/2005, come modificati dal d.lgs. 217/2017.

[8] Le linee guida, approvate dall'Agenzia per l'Italia Digitale (AgID) con determinazione n. 407/2020 del 9 settembre 2020, abrogano le precedenti regole tecniche in materia di documenti informatici (d.p.c.m. 13 novembre 2014, pubblicato in G.U. 12 gennaio 2015, n. 8), le regole tecniche in materia di sistema di conservazione e, fatte salve alcune disposizioni, le regole tecniche per il protocollo informatico (entrambi d.p.c.m. 3 dicembre 2013, pubblicati in G.U. 12 marzo 2014, n. 59). Le modifiche e le integrazioni sono state adottate dall'AgID con determinazione n. 371/2021 del 17 maggio 2021: l'applicazione e il correlato obbligo di adozione delle linee guida e dei relativi allegati, inizialmente fissati per la data del 7 giugno 2021, sono stati posticipati al 1° gennaio 2022.

carattere tecnico, fondamentali per l'attuazione delle disposizioni di rango primario[9]: le regole tecniche, a seguito delle modifiche introdotte dal d.lgs. 217/2017, sono costituite da linee guida adottate dall'Agenzia per l'Italia Digitale (AgID) secondo il procedimento previsto nell'art. 71 del d.lgs. 82/2005, invece che da decreti del Presidente del Consiglio dei ministri o del Ministro delegato come in passato[10]. Al riguardo il Consiglio di Stato ha chiarito la valenza *erga omnes* e il carattere di vincolatività delle regole tecniche, da qualificare come "atti di regolazione seppur di natura tecnica" sotto il profilo della gerarchia delle fonti, soggette al sindacato del giudice amministrativo[11].
Le modifiche del Codice dell'amministrazione digitale nel corso degli anni si sono rese necessarie anche in considerazione dell'evoluzione normativa a livello europeo; in particolare, con il d.lgs. 179/2016 e il d.lgs. 217/2017, le disposizioni del d.lgs. 82/2005 sono state adeguate proprio al regolamento (UE) eIDAS n. 910/2014[12], che reca disposizioni rilevanti in materia di documenti informatici, firme elettroniche e sigilli elettronici[13].
Al riguardo è necessaria una premessa in merito all'ambito di applicazione della disciplina oggetto di analisi. Infatti, ai sensi dell'art. 2, d.lgs. 82/2005, le disposizioni del Codice e le relative linee guida che regolano l'attività documentale in ambito digitale e riguardano il documento informatico, le firme elettroniche e i servizi fiduciari, la riproduzione e la conservazione dei documenti, l'identità digitale, il domicilio digitale e

[9] Artt. 20, c. 3, e 71, d.lgs. 82/2005. Cfr. A. Maggipinto, *Amministrazione digitale*, in M. Durante – U. Pagallo (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, 2012, 283 ss., che rileva come in ambito pubblico norma e tecnica siano quanto mai legate da un doppio filo, in quanto i principi giuridici guidano l'innovazione e le regole tecniche possono realizzarla; M. Martoni, *Il documento informatico e le firme elettroniche nel Codice dell'amministrazione digitale*, in C. Di Cocco – G. Sartor (a cura di), *Temi di diritto dell'informatica*, IV ed., Torino, 2020, 41, che sottolinea la duplice funzione delle regole tecniche, che consiste, da una parte, nel dettare indicazioni di dettaglio e, dall'altra, nel garantire al Codice dell'amministrazione digitale l'aggiornamento rispetto all'evoluzione tecnologica.

[10] Le linee guida sono adottate dall'AgID, previa consultazione pubblica da svolgersi entro trenta giorni, sentite le amministrazioni competenti, sentito il Garante per la protezione dei dati personali e acquisito il parere della Conferenza Unificata; divengono efficaci dopo la pubblicazione nell'apposita area del sito istituzionale dell'AgID e ne è data notizia nella Gazzetta Ufficiale della Repubblica italiana. Al riguardo rileva il regolamento per l'adozione di linee guida per l'attuazione del Codice dell'amministrazione digitale, adottato dall'AgID con determinazione n. 160 del 17 maggio 2018. Le regole tecniche precedentemente approvate con d.p.c.m. restano efficaci fino all'eventuale modifica o abrogazione da parte delle linee guida di cui all'art. 71, d.lgs. 82/2005, come modificato dal d.lgs. 217/2017 (art. 65, c. 10, d.lgs. 217/2017).

[11] Parere del Consiglio di Stato n. 2122 del 10 ottobre 2017 sullo schema del d.lgs. 217/2017, che nella gerarchia delle fonti inquadra le linee guida come atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute; le garanzie procedimentali e il più forte rispetto di criteri di "legalità procedimentale" compensano la maggiore flessibilità del principio di legalità sostanziale.

[12] Dal momento che si tratta di un regolamento europeo, le disposizioni sono comunque direttamente applicabili in ciascuno degli Stati membri.

[13] Le firme sono create dalle persone fisiche e i sigilli dalle persone giuridiche, per garantire l'origine e l'integrità dell'insieme di dati che costituiscono il documento cui sono apposti; i sigilli elettronici sono disciplinati nell'art. 35 ss., reg. (UE) n. 910/2014 e si differenziano (come le firme) in semplici, avanzati e qualificati.

la trasmissione telematica dei documenti[14] si applicano non solo all'ambito pubblico[15], ma anche ai privati, ove non diversamente previsto, e, di conseguenza, ai rapporti di natura privatistica, integrandosi nell'ordinamento civilistico[16]. Di conseguenza ciò si traduce nella peculiare convivenza di disposizioni afferenti a diversi rami del diritto (norme civilistiche e amministrative) nello stesso atto normativo, il Codice dell'amministrazione digitale[17].

3. Dalla *res signata* al documento informatico

All'esteso ambito di applicazione a livello soggettivo corrisponde un'ampia estensione della definizione normativa di documento informatico a livello oggettivo.
Il documento informatico è definito ampiamente come il documento elettronico, che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti[18].
La definizione è stata integrata con il riferimento al documento elettronico, ossia qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva[19], al fine di adeguarla alle disposizioni del reg. (UE) n. 910/2014; infatti ai sensi dell'art. 1, c. 1-*bis*, d.lgs. 82/2005 «ai fini del […] Codice, valgono le definizioni di cui all'articolo 3 del Regolamento eIDAS».
La definizione di documento analogico è ricavata in negativo e consiste nella rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti[20].
Le definizioni normative di documento informatico e analogico conseguono alla necessità di fornire una definizione al documento informatico. Prima dell'avvento delle tecnologie l'ordinamento giuridico italiano era privo di una definizione di carattere generale di documento, seppur diverse norme già regolamentassero l'attività di documentazione; la definizione di documento è stata elaborata dalla dottrina[21].
Il documento analogico è formato da una componente materiale (*res signata*), esito dell'attività di un soggetto che, con mezzi idonei, ha modificato la materia, in modo da consentire la rappresentazione di un fatto o di un atto, e di una componente immateriale, che porta a distinguere documenti dichiarativi (manifestazioni di pensiero o di volontà volte a produrre effetti giuridici) e narrativi (mere esposizioni di un fatto);

[14] In specifico il capo II, gli artt. 43 e 44 del capo III, il capo IV, gli artt. 3-*bis* e 64, d.lgs. 82/2005.

[15] Art. 2, c. 2, d.lgs. 82/2005: in specifico le pubbliche amministrazioni di cui all'art. 1, c. 2, d.lgs. 165/2001, nel rispetto del riparto di competenza di cui all'art. 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché le autorità amministrative indipendenti di garanzia, vigilanza e regolazione, i gestori di servizi pubblici, comprese le società quotate, e le società a controllo pubblico, escluse in tal caso le società quotate.

[16] Art. 2, c. 3, d.lgs. 82/2005.

[17] M. Guernelli, *Il quadro normativo italiano*, in G. Finocchiaro – F. Delfini (a cura di), *Diritto dell'informatica*, Torino, 2014, 109 ss.

[18] Art. 1, c. 1, lett. *p)*, d.lgs. 82/2005.

[19] Art. 3, par. 1, n. 35), reg. (UE) n. 910/2014.

[20] Art. 1, c. 1, lett. *p-bis)*, d.lgs. 82/2005.

[21] M. Martoni, *Il documento informatico e le firme elettroniche nel Codice dell'amministrazione digitale*, cit., 28 ss.

il documento può essere pubblico (atto pubblico) o privato (scrittura privata)[22]. Dal momento che la materia più diffusa è la carta, capace di rendere stabile e immodificabile il contenuto documentale, il più diffuso è il documento cartaceo: sotto tale profilo le caratteristiche del supporto materiale, la carta, hanno finito per creare una sorta di legame indissolubile tra il documento e il supporto cartaceo[23].

Nel passaggio dalla *res signata* al documento informatico il contenuto documentale si distacca e abbandona i limiti del supporto materiale, percepibile e tangibile, dal momento che consiste in una sequenza di valori binari ed è il risultato di un'elaborazione informatica; di conseguenza può essere formato in molteplici modi[24]. La formazione del documento informatico, infatti, avviene con modalità eterogenee, che mostrano l'ampia estensione del concetto:

la creazione tramite l'utilizzo di strumenti software o servizi *cloud* qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità;

l'acquisizione di un documento informatico per via telematica o su supporto informatico, l'acquisizione della copia per immagine su supporto informatico di un documento analogico, l'acquisizione della copia informatica di un documento analogico[25];

la memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;

la generazione o il raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma

[22] Sul documento cfr., *inter alia*, F. Carnelutti, *Documento (teoria moderna)*, in *Novissimo Digesto Italiano*, vol. VI, Torino, 1957, 85 ss.; A. Candian, *Documentazione e documento (teoria generale)*, in *Enciclopedia del diritto*, vol. XIII, Milano, 1964, 579 ss.; N. Irti, *Sul concetto giuridico di documento*, in *Rivista trimestrale di diritto e procedura civile*, 1969, 484 ss.; S. Patti, *Documento*, in *Digesto delle Discipline Privatistiche*, sezione civile, VII, Torino, 1991. Sul documento informatico cfr., *inter alia*, E. Giannantonio, *Il valore giuridico del documento elettronico*, in *Rivista del diritto commerciale e del diritto generale delle obbligazioni*, 9-12, parte 1, 1986, 261 ss.; G. Finocchiaro, *Documento informatico e firma digitale*, in *Contratto e impresa*, 2, 1998, 956 ss.; G. Rognetta, *La firma digitale e il documento informatico*, Napoli, 1999; A. Masucci, *Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, in *Rivista di diritto civile*, 5, 2004, 749 ss.; M. Martoni, *Il documento informatico e le firme elettroniche nel Codice dell'amministrazione digitale*, cit., 28 ss.

[23] G. Pascuzzi (a cura di), *Il diritto dell'era digitale*, cit., 115 ss.

[24] Il documento informatico è tale solo all'interno di un sistema informatico e ciò che è visibile su uno schermo ne è solo la rappresentazione, come la stampa cartacea ne è una riproduzione; cfr. M. Martoni, *Il documento informatico e le firme elettroniche nel Codice dell'amministrazione digitale*, cit., 42 ss.

[25] La copia informatica di documento analogico è «il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto»; la copia per immagine su supporto informatico di documento analogico è «il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto»; la copia informatica di documento informatico è «il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari»; il duplicato informatico è «il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario» (art. 1, c. 1, lett. *i-bis)*, *i-ter)*, *i-quater)*, *i-quinquies)*, d.lgs. 82/2005). Le copie informatiche di documenti analogici, le copie analogiche di documenti informatici, le copie informatiche di documenti informatici e i duplicati sono disciplinati dall'art. 22 ss., d.lgs. 82/2005, che si occupano di regolare il passaggio da analogico a digitale e viceversa.

statica[26].
Il documento informatico "si libera" del supporto materiale e ciò consente di trasferire la rappresentazione informatica da un supporto all'altro generando duplicati e copie; in ogni caso, come emerge anche dalle modalità di formazione dello stesso, è opportuno precisare che anche il documento informatico necessita di un'incorporazione su base materiale, ossia di un supporto informatico in sostituzione del tradizionale supporto cartaceo e, di conseguenza, non deve considerarsi superato l'elemento della materialità, seppur si atteggi in modo sensibilmente diverso[27].
Il documento informatico, anche privo di sottoscrizione, possiede un proprio valore giuridico[28], ma la firma elettronica costituisce strumento di identificazione [29] e imputazione del documento e delle dichiarazioni in esso contenute al firmatario con le connesse conseguenze giuridiche. Per tali ragioni la firma elettronica costituisce elemento centrale della disciplina in materia; il valore giuridico e l'efficacia probatoria di un documento informatico, infatti, variano in base alla tipologia di firma elettronica utilizzata.

4. Firma autografa e firma elettronica

Al passaggio dal documento cartaceo, quale oggetto materiale percepibile e tangibile, *res signata*, al documento informatico corrisponde il passaggio dalla firma autografa a quella elettronica, che parimenti mostrano rilevanti tratti differenziali[30].
La firma autografa si presenta come un segno apposto manualmente sul documento cartaceo e direttamente riconducibile al soggetto: è legata al supporto fisico del documento, valutabile in modo diretto e dotata in sé di validità temporale illimitata. Diversamente, la firma elettronica consiste in una sequenza binaria riconducibile al soggetto solo attraverso una procedura informatica: è legata in modo indissolubile al contenuto del documento, valutabile solo con mezzi informatici e dotata di una validità temporale limitata; la firma elettronica si riferisce al procedimento informatico che permette

[26] Così il paragrafo 2.1.1. delle linee guida adottate dall'AgID.

[27] Cfr. F. Ricci, voce *Documento informatico*, in *Il diritto*, *Enciclopedia de Il Sole 24 ore*, Milano, 2007; E. Tucci, *I principali strumenti del codice dell'amministrazione digitale*, in G. Cassano (a cura di), *L'informatica per il giurista*, Santarcangelo di Romagna, 2019, 165 ss.

[28] Art. 20, c. 1-*bis*, d.lgs. 82/2005.

[29] L'art. 3, par. 1, n. 1), reg. (UE) n. 910/2014 definisce l'identificazione elettronica come «il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica» e l'art. 3, par. 1, n. 5), reg. (UE) n. 910/2014 definisce l'autenticazione come «un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure l'origine e l'integrità di dati in forma elettronica». Nell'ordinamento italiano, invece, l'autenticazione non è più riferita al soggetto che accede al sistema informatico, ma al documento informatico; cfr. G. Finocchiaro, *Una prima lettura del Reg. UE n. 910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari*, cit., 422 ss.

[30] Al riguardo, è opportuno specificare che sono molto limitati i casi in cui è richiesta solo la forma analogica; è il caso del testamento olografo ai sensi dell'art. 602 c.c., che non può essere redatto con strumenti informatici, giacché deve essere redatto dal testatore di proprio pugno.

di accertare la paternità di un documento informatico[31].
In relazione al documento la firma assolve funzioni di particolare rilievo, quali la funzione indicativa, identificando il soggetto; la funzione dichiarativa, consentendo l'assunzione di paternità e l'imputazione delle dichiarazioni che ne formano il contenuto al firmatario; la funzione probatoria, permettendo di provare la provenienza del documento, dal momento che costituisce mezzo di prova[32].
Secondo una classificazione comune, i metodi di identificazione utilizzati nelle diverse firme elettroniche possono essere individuati nelle tre categorie "*something you know*", "*something you are*", "*something you have*", a seconda che il meccanismo di identificazione si basi sulle conoscenze dell'utente (come la conoscenza di un codice, di una parola chiave o di un numero di identificazione personale), sulle caratteristiche fisiche dell'utente (è il caso della firma grafometrica) o sul possesso di un oggetto da parte dell'utente (come un dispositivo quale una *smart card* o un *token*)[33].

5. I principi di neutralità tecnologica e non discriminazione

La disciplina del documento informatico e delle firme elettroniche, scaturente dal regolamento europeo eIDAS e dalla disciplina nazionale, è pervasa dal principio di non discriminazione, che accompagna l'altro criterio fondamentale costituito dal principio di neutralità tecnologica.
Il principio di non discriminazione è previsto dal regolamento europeo eIDAS n. 910/2014 in riferimento ai diversi "snodi" dell'attività documentale, dal momento che riguarda i documenti elettronici, le firme elettroniche, i sigilli elettronici, la validazione temporale elettronica e i servizi elettronici di recapito certificato[34]. In specifico il principio di non discriminazione degli strumenti digitali rispetto a quelli analogici si traduce, nel caso dei documenti (art. 46), nel non poter negare a un documento elettronico «gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica» e, nel caso delle firme (art. 25), nel non poter negare a una firma elettronica «gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica o perché non

[31] L'art. 3, par. 1, n. 9), reg. (UE) n. 910/2014 definisce firmatario «una persona fisica che crea una firma elettronica». Cfr. G. Finocchiaro, *Firme elettroniche e firma digitale*, cit., 310. In merito M. Martoni, *Il documento informatico e le firme elettroniche nel Codice dell'amministrazione digitale*, cit., 28 ss. rileva che la sottoscrizione è il meccanismo tradizionale con cui un soggetto fa propria una dichiarazione scritta, assumendosene la paternità, ma non è di per sé sufficiente a garantire la titolarità dello scritto e, sotto tale profilo, esistono espedienti giuridici atti a conferire maggiore certezza, quali il riconoscimento espresso, il riconoscimento tacito o mancato disconoscimento e l'autenticazione della sottoscrizione.

[32] Cfr. M. Martoni, *Il documento informatico e le firme elettroniche nel Codice dell'amministrazione digitale*, cit., 32, che ricorda come le tipiche funzioni della firma (identificativa, dichiarativa e probatoria) nell'era analogica trovavano esplicazione nelle qualità intrinseche del supporto cartaceo. In merito cfr. A.C. Amato Mangiameli, *Informatica giuridica. Appunti e materiali ad uso di lezioni*, cit., 270 ss.

[33] Cfr. G. Finocchiaro, *Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale*, in *Contratto e impresa*, 2, 2011, 497.

[34] Artt. 25, 35, 41, 43 e 46 e i considerando 49 e 63, reg. (UE) n. 910/2014.

soddisfa i requisiti delle firme elettroniche qualificate». Di conseguenza non possono essere discriminati gli strumenti digitali (documenti informatici e firme elettroniche) rispetto a quelli analogici e neppure alcune tipologie di firme (firma elettronica semplice) rispetto ad altre (firma elettronica qualificata).

Riguardo alle firme elettroniche, posto il principio di non discriminazione, ai sensi del considerando 49 del regolamento eIDAS, «spetta al diritto nazionale definire gli effetti giuridici delle firme elettroniche, fatto salvo per i requisiti previsti dal […] regolamento secondo cui una firma elettronica qualificata dovrebbe avere un effetto giuridico equivalente a quello di una firma autografa»[35].

Il principio di neutralità sotto il profilo tecnologico è previsto nel considerando 27 del reg. (UE) n. 910/2014, che ritiene auspicabile che gli effetti giuridici prodotti dal regolamento «siano ottenibili mediante qualsiasi modalità tecnica, purché siano soddisfatti i requisiti da esso previsti». In ossequio a tale principio il diritto deve rimanere neutro rispetto alla tecnologia senza riferirsi a livelli di sicurezza predeterminati o a tecnologie specifiche, limitandosi ad individuare l'obiettivo da perseguire senza indicare le modalità tecniche per perseguirlo. Il principio di neutralità tecnologica, che pervade la normativa europea e nazionale, si collega alla necessità di tutelare la concorrenza tra gli operatori di mercato, rispettare l'autonomia, garantire maggiore effettività e permettere l'adeguamento all'evoluzione tecnologica[36].

Prima della direttiva 1999/93/CE il nostro ordinamento conosceva solo la firma digitale, introdotta dal d.p.r. 513/1997; il concetto di firma elettronica, di origine europea, trova fondamento proprio nel principio di neutralità tecnologica[37].

Le norme europee e nazionali, pertanto, identificano nelle tecnologie informatiche uno strumento atto a realizzare gli obiettivi che si prefiggono, garantendo però l'autonomia nella scelta della tecnologia da impiegare, espressione del principio di neutralità tecnologica; non viene normativamente imposta alcuna soluzione tecnologica determinata, prevedendo il criterio di libertà nella scelta e il principio di non discriminazione tra strumenti analogici e digitali e tra tecnologie diverse.

Al riguardo è opportuno precisare che in materia di documenti informatici e firme elettroniche un ruolo fondamentale è svolto dall'*United Commission on International Trade Law* (UNCITRAL), la cui azione si è basata proprio sui principi di neutralità tecnologica, non discriminazione ed equivalenza funzionale[38].

---

[35] Cfr. A. Gentili, *Negoziare* on line *dopo la riforma del codice dell'amministrazione digitale*, in *Il Corriere del merito*, 4, 2011, 353 ss., secondo cui il diritto interno non mette in questione la capacità di valere del documento elettronico, ma la capacità di valere come scritto.

[36] G. Finocchiaro, *Diritto di Internet*, III ed., Bologna, 2020, 88 ss.

[37] Cfr. M. Martoni, *Il documento informatico e le firme elettroniche nel Codice dell'amministrazione digitale*, cit., 44 ss.

[38] Il principio di equivalenza funzionale si basa sull'analisi delle funzioni che svolge il documento cartaceo, al fine di determinare in che modo tali funzioni possano essere ugualmente soddisfatte attraverso gli strumenti elettronici; così G. Finocchiaro – Hu Guiping, *Norme sulle firme elettroniche a confronto: UE, Italia e Cina*, in *MediaLaws – Rivista di diritto dei media*, 2, 2021, 18 ss. In merito, cfr., altresì, G. Finocchiaro, *Diritto di Internet*, cit., 91 ss.

6. Firme elettroniche: valore giuridico e probatorio

La normativa delinea un sistema di sottoscrizioni a più livelli, con diversa forza giuridica e probatoria, in relazione alle diverse caratteristiche tecniche che le connotano: la conseguente distinzione tra tipologie di firma si basa sulla diversa capacità di garantire sicurezza e affidabilità a livello tecnologico circa l'identità dei soggetti e l'integrità dei dati. Le differenti caratteristiche tecniche influiscono sulla certezza nella riconducibilità della dichiarazione al firmatario e sul rischio che sia alterato il documento[39].
Il diritto, pertanto, prevede un sistema graduale del valore giuridico e probatorio delle firme che consegue direttamente alle caratteristiche tecniche e si serve delle diverse tecnologie disponibili per raggiungere l'obiettivo di assicurare la certezza delle relazioni giuridiche[40].
Negli anni la normativa è stata oggetto di modifiche e integrazioni relative alle firme elettroniche, al fine di semplificarne l'adozione e l'uso, garantirne un utilizzo diffuso e superare le inerzie al riguardo, in particolare da parte delle pubbliche amministrazioni[41]. Tra i diversi interventi di riforma, il d.lgs. 179/2016 e il d.lgs. 217/2017 hanno adeguato la normativa italiana alle disposizioni del regolamento (UE) n. 910/2014 e, di conseguenza, hanno modificato e integrato il d.lgs. 82/2005.
L'impatto del regolamento eIDAS provoca effetti anche sulle regole tecniche in materia, che devono parimenti essere aggiornate: al riguardo si applicano le linee guida e, in caso non siano ancora state prodotte e pubblicate, le regole tecniche vigenti restano efficaci fino all'adozione delle stesse[42]. In materia al momento sono state pubblicate soltanto le linee guida contenenti le regole tecniche e le raccomandazioni afferenti alla generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate (pubblicate il 20 giugno 2019) e le linee guida per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD (pubblicate il 23 aprile 2020); di conseguenza, nelle more della produzione delle regole tecniche mancanti, per quanto non disciplinato, si deve fare riferimento alle regole tecniche vigenti in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali (d.p.c.m. 22 febbraio 2013, pubblicato in G.U. 21 maggio 2013, n. 117).

[39] Cfr. O. Troiano, *Firma e forma elettronica: verso il superamento della forma* ad substantiam. *Riflessioni a margine del regolamento UE n. 910/2014 e delle recenti riforme del codice dell'amministrazione digitale*, in *La Nuova giurisprudenza civile commentata*, 1, 2018, 87 ss., secondo cui il punto dell'affidabilità diventa quindi la discriminante più evidente nell'atteggiamento del legislatore quando disciplina la firma elettronica rispetto all'approccio tradizionalmente tenuto nel disciplinare la forma scritta.

[40] Cfr. G. Pascuzzi (a cura di), *Il diritto dell'era digitale*, cit., 113 ss.; M. Martoni, *Il documento informatico e le firme elettroniche nel Codice dell'amministrazione digitale*, cit., 27 ss.: «la normativa, nel determinare gli effetti ed il valore giuridico del documento informatico, sia esso sottoscritto o meno, si sofferma sugli aspetti più strettamente tecnici che caratterizzano le diverse tipologie di firma elettronica, riconoscendo uno specifico rilievo giuridico proprio quale diretta conseguenza delle diverse implementazioni tecniche».

[41] Secondo A. Gentili, *Negoziare* on line *dopo la riforma del codice dell'amministrazione digitale*, cit., 353 la versione originaria del d.lgs. 82/2005 aveva frenato più che incentivato il ricorso ad atti giuridici digitali, a causa dell'incertezza sulla validità del requisito della forma scritta e sulla forza probatoria delle firme più "deboli", unita alla maggiore complessità e al più alto costo della firma "forte", la firma digitale; tali motivazioni sono all'origine delle modifiche incisive del d.lgs. 235/2010.

[42] Art. 65, c. 10, d.lgs. 217/2017.

Al fine di esaminare la disciplina relativa ai documenti informatici e alle firme elettroniche, in premessa è necessario osservare che, in merito al valore del documento, vige nell'ordinamento il principio della libertà della forma nella manifestazione della volontà negoziale (art. 1325 c.c.), ma in numerosi casi è imposta la forma scritta *ad substantiam* (per la validità dell'atto, ossia per la produzione degli effetti giuridici) o *ad probationem* (per la prova di un atto o un fatto, ossia per la dimostrazione degli effetti giuridici). È il caso dell'art. 1350 c.c., che impone in determinate fattispecie la forma scritta a pena di nullità; gli atti previsti dalla disposizione «devono farsi per atto pubblico o per scrittura privata, sotto pena di nullità». La forma scritta è richiesta dall'ordinamento, limitando l'autonomia privata, in relazione a fattispecie che, per rilevanza economica e conseguenze giuridiche, necessitano di una particolare attenzione da parte dei contraenti e che esigono maggiore certezza[43].

Di conseguenza, è necessario verificare quali soluzioni di firma elettronica conferiscono al documento informatico l'attitudine a integrare e assolvere il requisito della forma scritta ed il relativo valore probatorio.

In caso di documento informatico privo di sottoscrizione, l'idoneità a soddisfare il requisito della forma scritta e il valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche oggettive di sicurezza, integrità e immodificabilità[44]; il documento, quindi, anche in tal caso possiede un proprio valore giuridico, in conformità al principio cardine di non discriminazione di cui all'art. 46 del regolamento (UE) eIDAS n. 910/2014.

Sono quattro le tipologie di firma elettronica previste dalla normativa nazionale di riferimento, che recano differenze relative alla validità giuridica e all'efficacia probatoria: firma elettronica semplice, firma elettronica avanzata, firma elettronica qualificata e firma digitale; le prime tre firme sono definite e disciplinate a livello sovranazionale dal regolamento europeo eIDAS n. 910/2014, richiamato dal d.lgs. 82/2005, mentre la firma digitale è definita e disciplinata dal nostro ordinamento nel Codice dell'amministrazione digitale[45].

6.1. La firma elettronica semplice

La firma elettronica cosiddetta semplice consiste in «dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare»[46]. Si tratta quindi di uno strumento che consente di associare

[43] A. Maggipinto, *Amministrazione digitale*, cit., 292 ss. sottolinea come il codice civile prediliga il documento scritto, confinando a casi residuali le forme di documentazione diverse, a causa della maggiore certezza che è in grado di fornire.

[44] Art. 20, c. 1-*bis*, d.lgs. 82/2005.

[45] Al riguardo O. Troiano, *Firma e forma elettronica: verso il superamento della forma* ad substantiam. *Riflessioni a margine del regolamento UE n. 910/2014 e delle recenti riforme del codice dell'amministrazione digitale*, cit., 79 ss. evidenzia che, a fronte della tripartizione definitoria, il regolamento eIDAS offre un'articolata disciplina degli effetti giuridici solo della firma elettronica e della firma elettronica qualificata.

[46] Art. 3, par. 1, n. 10), reg. (UE) n. 910/2014; la definizione, prima contenuta nell'art. 1, lett. *q)*, d.lgs. 82/2005, è stata abrogata dal momento che nell'ordinamento valgono le definizioni di cui

un insieme di dati elettronici, quali quelli che costituiscono il documento, a un identificativo unico, costituito appunto dalla firma elettronica; è il caso di una *password* o di un codice *pin*.

Si tratta della firma "debole" o "leggera" nell'ordinamento, dal momento che in tal caso l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili *ex post* dal giudice, tenuto conto delle caratteristiche di sicurezza, integrità e immodificabilità. Pertanto il documento su cui è apposta una firma elettronica semplice ha lo stesso valore del documento informatico non sottoscritto e non fornisce certezza *a priori* agli utilizzatori, giacché il legislatore non attribuisce *ex ante* un valore specifico al documento e rimette la valutazione in merito *a posteriori* al giudice[47].

La firma elettronica semplice risponde ai principi di non discriminazione e neutralità tecnologica, dal momento che il legislatore non prescrive caratteristiche tecniche specifiche o un livello di sicurezza predeterminato; la norma sostanzialmente si limita a ribadire il principio di non disconoscimento e non discriminazione che governa la disciplina.

In tali casi il giudice dovrà ponderare attentamente valore ed efficacia, con una valutazione caso per caso, fondata sulle caratteristiche del documento informatico, ossia sicurezza, integrità e immodificabilità.

Alla luce del ruolo attribuito dalla norma al giudice nella valutazione del valore giuridico e probatorio del documento, è significativa la giurisprudenza sull'efficacia probatoria dell'email quale firma elettronica semplice; nelle sentenze la valutazione del valore della posta elettronica, normativamente rimessa al giudice, ha determinato esiti molto diversi confermando, di conseguenza, che si tratta di uno strumento che non fornisce certezza preventiva agli utilizzatori, a differenza delle altre tipologie di firma elettronica[48].

Al riguardo è interessante la sentenza del Tribunale di Milano, sez. V, 18 ottobre 2016, n. 11402 per il fatto che tratta del valore dell'email alla luce delle disposizioni europee e nazionali, richiamando esplicitamente il principio di non discriminazione; il caso riguarda l'opposizione a decreto ingiuntivo emesso per il pagamento di fatture per compensi di un contratto di collaborazione in materia di grafica e informatica da parte di una società contro un collaboratore[49].

Il Tribunale di Milano dichiara che «è ammissibile come prova il documento elettroni-

all'art. 3, reg. (UE) n. 910/2014, come previsto nell'art. 1, c. 1-*bis*, d.lgs. 82/2005. Tale considerazione vale anche per le altre definizioni del reg. (UE) n. 910/2014, richiamate di seguito, che si applicano direttamente nell'ordinamento italiano e hanno portato all'abrogazione di varie definizioni del CAD.

[47] Art. 20, c. 1-*bis*, d.lgs. 82/2005, come modificato dal d.lgs. 179/2016 e dal d.lgs. 217/2017, che disciplina sia il caso del documento privo di firma, sia il caso del documento cui è apposta la firma elettronica semplice.

[48] Al riguardo cfr. F. Ricci, *L'efficacia probatoria dell'e-mail non sottoscritta*, in *Rivista Trimestrale di Diritto e Procedura Civile*, 2, 2021, 629 ss.

[49] Nel caso la società eccepisce che spetti alla controparte, il collaboratore, provare le sue prestazioni e che l'email di un socio accomandatario della società attrice non si possa considerare documento valido, in quanto non sottoscritto. Il Tribunale di Milano, che respinge l'opposizione, esamina il valore giuridico dell'email dell'accomandatario della società attrice, che per i contenuti recati conferma l'esistenza del debito a carico della parte attrice e le relative difficoltà a pagarlo.

co anche in assenza di firma elettronica qualificata» e motiva l'affermazione alla luce del quadro giuridico europeo e nazionale di riferimento e, in particolare, del principio di non discriminazione, di cui agli articoli 25 e 46 del regolamento (UE) n. 910/2014. Il Tribunale individua nel caso dell'email un'ipotesi di firma elettronica[50]: «la spedizione da un indirizzo riferibile ad una certa società d'azienda deve essere ritenuta firma elettronica»; infatti, nel caso dell'email si utilizzano le credenziali di accesso alla relativa casella. L'utilizzo di una casella di posta elettronica recante chiaramente il riferimento alla persona, unitamente al contenuto, indicano che quelle parole contenute nell'email sono riferibili al soggetto.

Il Tribunale di Milano è ben consapevole che nel caso dell'email si tratta di «caratteri facilmente modificabili, ad opera di chiunque avesse accesso alla casella di posta o anche successivamente», ma rileva come la parte attrice non abbia presentato uno specifico disconoscimento, ipotizzando l'intervenuta modifica; peraltro, dalle risultanze l'email risulta pienamente confermata. Secondo il Tribunale, un documento informatico accompagnato da una firma elettronica semplice ha piena dignità probatoria, salvo il potere e dovere del giudice di valutarlo ai sensi di quanto previsto dalle norme.

In direzione analoga alla sentenza del Tribunale di Milano si colloca l'ordinanza della Corte di Cassazione, sez. VI civile, 14 maggio 2018, n. 11606 relativa a un decreto ingiuntivo per importi relativi al pagamento di strumentazioni di navi da diporto, provati dallo scambio di email. Secondo la Corte di Cassazione, ai sensi del d.lgs. 82/2005, l'e-mail costituisce un documento informatico e «forma piena prova dei fatti e delle cose rappresentate, se colui contro il quale viene prodotta non ne disconosca la conformità ai fatti o alle cose medesime»[51].

Sul valore della posta elettronica è interessante però anche la giurisprudenza che si orienta in senso diverso; è il caso della sentenza della Corte di Cassazione, sez. lavoro, 8 marzo 2018, n. 5523, che confermando la sentenza impugnata, ha ritenuto illegittimo il licenziamento di un lavoratore fondato sulla corrispondenza relativa all'indirizzo di posta elettronica del dipendente, dovendosi escludere che i messaggi siano riferibili al suo autore apparente, trattandosi di email prive di firma elettronica[52]. La Corte di

[50] Art. 3, c. 1, n. 10), reg. (UE) n. 910/2014.

[51] Al riguardo la Corte di Cassazione conferma la Corte d'Appello di Milano, 29 novembre 2016, n. 4448, che a sua volta aveva confermato la sentenza del Tribunale di Milano del 15 gennaio 2016, ritenendo che il contratto di fornitura di beni, il relativo rapporto commerciale tra le parti e il conseguente credito azionato fossero stati provati da uno scambio di email tra le società coinvolte nell'operazione, nel quale la società acquirente aveva proposto un piano di rientro per i crediti scaduti, accettato dalla società alienante. Nella fattispecie, in considerazione della mancata corresponsione del prezzo, la società venditrice depositava presso il Tribunale di Milano ricorso per decreto ingiuntivo per il recupero delle somme dovute, avverso il quale l'acquirente proponeva opposizione, eccependo il parziale pagamento delle somme dovute. Per tali motivi, il Tribunale di Milano revocava il decreto ingiuntivo, confermava come dovute le restanti somme e condannava l'opponente al pagamento dell'importo residuo; la Corte d'Appello aveva confermato il primo grado. Nel caso specifico oggetto di pronuncia la società si era impegnata nell'email a rientrare dalla propria esposizione debitoria e, pertanto, in modo conforme a quanto espresso dalla Corte d'Appello di Milano, la Corte di Cassazione ritiene dimostrata l'esistenza del rapporto contrattuale, nonché verificato l'importo del credito azionato col decreto ingiuntivo.

[52] La vicenda riguardava la contestazione al lavoratore, dirigente e responsabile di un'area territoriale, di una condotta irregolare in merito all'applicazione della procedura cosiddetta "rivalutazioni di magazzino" che, secondo le indagini aziendali, aveva portato all'accredito di somme non dovute in favore di alcune società commerciali partner, in quanto relative a giacenze di prodotti di telefonia

Cassazione evidenzia che in relazione all'efficacia probatoria dei documenti informatici l'art. 20 del d.lgs. 82/2005 attribuisce l'efficacia prevista dall'art. 2702 c.c. solo al documento sottoscritto con firma elettronica avanzata, qualificata o digitale, mentre è liberamente valutabile dal giudice l'idoneità di ogni diverso documento informatico, come l'email tradizionale, a soddisfare il requisito della forma scritta, in relazione alle sue caratteristiche oggettive di sicurezza, integrità ed immodificabilità: secondo la Corte di Cassazione va escluso che i messaggi siano riferibili al suo autore apparente, in quanto, trattandosi di email prive di firma elettronica, i documenti non hanno la natura di scrittura privata prevista dall'art. 2702 c.c.[53].

In linea con la sentenza appena esaminata, l'ordinanza della Corte di Cassazione, sez. VI civile, 6 febbraio 2019, n. 3540, relativa a un risarcimento dei danni per diffamazione a mezzo email, afferma che l'email non ha l'efficacia della scrittura privata ed è liberamente valutabile in giudizio dal giudice, ribadendo la «circoscritta valenza probatoria del messaggio di posta elettronica privo di certificazione volta ad attestarne la provenienza dall'autore, che come tale è liberamente valutabile dal giudice» e richiamando la precedente sentenza n. 5223/2018[54].

Nello stesso senso la sentenza della Corte d'Appello di Roma, 26 ottobre 2020, n. 2110, secondo cui il messaggio di posta elettronica è un documento elettronico privo di firma contenente la rappresentazione informatica di fatti giuridicamente rilevanti e perciò ha l'efficacia probatoria tipica delle rappresentazioni meccaniche, dovendo essere ricondotto al caso delle riproduzioni informatiche di cui all'art. 2712 c.c. È, infatti, opportuno precisare che nelle sentenze esaminate l'email è ricostruita diversamente: in alcuni casi è qualificata come scrittura informatica (munita o meno di firma elettronica), in altri è individuata quale mera riproduzione informatica, ossia quale riproduzione meccanica, di cui all'art. 2712 c.c.: «Le riproduzioni fotografiche, informatiche o cinematografiche, le registrazioni fonografiche e, in genere, ogni altra rappresentazione meccanica di fatti e di cose formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità

mobile, in realtà non esistenti. Dopo il rigetto della domanda di impugnativa del licenziamento per giusta causa, che ne era scaturito, da parte del Tribunale di Roma con sentenza n. 721 del 2013, la Corte d'Appello di Roma con sentenza n. 5143 del 14 ottobre 2015, riformando la sentenza di primo grado, aveva dichiarato illegittimo il licenziamento in quanto, in difetto di riscontri certi a dimostrazione del diretto coinvolgimento del lavoratore nella procedura irregolare, la responsabilità che andava a configurarsi era di natura oggettiva, connessa cioè esclusivamente alla posizione dirigenziale ricoperta, osservando che la prospettazione della parte datoriale era fondata su messaggi di posta elettronica di "dubbia valenza probatoria" nonché su dichiarazioni provenienti da soggetti direttamente coinvolti nella vicenda e quindi inattendibili perché interessati ad un certo esito della lite.

[53] Cfr. F. Carpi, *Nuove tecnologie e prove*, in *Rivista Trimestrale di Diritto e Procedura Civile*, 1, 2021, 43 ss.

[54] La vicenda riguardava un risarcimento dei danni per diffamazione a mezzo email, accolto in primo grado con pronuncia confermata in appello, dal momento che risultava accertato che le email diffamatorie erano state inviate dall'indirizzo di posta elettronica della parte in causa; la Corte di Cassazione rigetta il ricorso in considerazione della corretta valutazione in appello di tutto il materiale probatorio, ma si sofferma sul valore dell'email. Sulla giurisprudenza esaminata, V. Colarocco – M. Cogode, *L'efficacia probatoria della mail non certificata*, in *Diritto di Internet*, 2, 2020, 373 ss. ritengono che secondo l'orientamento maggioritario (Corte di Cassazione nn. 5523/2018 e 5141/2019) l'email non ha l'efficacia probatoria della scrittura privata ai sensi dell'art. 2702 c.c., mentre secondo l'orientamento minoritario (Tribunale di Milano n. 11402/2016 e Corte di Cassazione n. 11606/2018) l'email è ammissibile come prova ai sensi dell'artt. 2702 c.c. anche in assenza di firma avanzata, qualificata o digitale.

ai fatti o alle cose medesime»[55].

Non solo l'email ha destato l'attenzione della giurisprudenza, ma altresì lo *short message service* (SMS)[56] o il messaggio WhatsApp[57], strumenti altrettanto diffusi, con interpretazioni anche in tal caso divergenti a seconda dei casi e della ricostruzione da parte del giudice.

In considerazione della mancata attribuzione di un valore predefinito *ex ante* dal legislatore al documento privo di sottoscrizione o accompagnato da una firma elettronica semplice emergono le oscillazioni giurisprudenziali nell'attribuzione di valore giuridico e probatorio ai particolari documenti costituiti da email, SMS e messaggi WhatsApp, strumenti di utilizzo frequente che possono venire in gioco in contesti giuridici diversi, quali nei casi oggetto di esame rapporti contrattuali, lavoro, relazioni interpersonali e possibili condotte illegittime, come nel caso della diffamazione: di conseguenza, l'attribuzione di efficacia probatoria può risultare determinante nella concreta tutela dei diritti.

6.2. La firma elettronica avanzata

La firma elettronica avanzata, introdotta nell'ordinamento con la riforma del d.lgs. 82/2005 recata dal d.lgs. 235/2010 e modificata dal d.lgs. 179/2016 e dal d.lgs. 217/2017, è una firma elettronica che «soddisfa i seguenti requisiti: a) è connessa

[55] Per approfondimenti cfr. F. Ricci, *L'efficacia probatoria dell'e-mail non sottoscritta*, cit., 629 ss., che condivisibilmente qualifica i messaggi di posta elettronica come uno strumento per compiere manifestazioni di volontà o di scienza, appartenendo pertanto, in relazione alla dichiarazione che tendono a realizzare, alla categoria delle scritture informatiche e non a quella delle mere riproduzioni informatiche. Secondo l'Autore, inoltre, l'inclusione dei dati dell'*account* del mittente in un messaggio di posta elettronica ha il valore sostanziale di una firma elettronica, essendo tali segni muniti del valore dichiarativo, indicativo e probatorio che contraddistingue un contrassegno di firma: può quindi intendersi come un mezzo utilizzato dall'autore del messaggio per firmarlo.

[56] Cfr. Corte d'Appello di Firenze, sez. lavoro, 5 luglio 2016, che ha accolto l'impugnazione del licenziamento verbale intimato con un messaggio SMS, negando l'idoneità in sé del messaggio SMS ad integrare il requisito della forma scritta necessario per intimare un recesso efficace; Cass. civ., sez. I, 17 luglio 2019, n. 19155, secondo cui, in relazione a un caso in cui il padre si accollava metà delle spese dell'asilo nido, poi tardivamente e genericamente contestate, l'SMS, riconducibile all'art. 2712 c.c., 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 rappresentate; Cass. civ., sez. II, 21 febbraio 2019, n. 5141, che ha respinto il ricorso di un soggetto che agiva per la restituzione di denaro sulla base della trascrizione di alcuni SMS, che erano stati disconosciuti: in tal caso l'SMS è stato inquadrato quale riproduzione informatica priva di firma ai sensi dell'art. 2712 c.c., che come tale fa piena prova se non ne è disconosciuta la conformità ai fatti o alle cose rappresentate.

[57] Cfr. Tribunale di Catania, 27 giugno 2017, che ha ritenuto efficace il licenziamento intimato dal datore di lavoro attraverso un messaggio WhatsApp, ritenendo assolto il requisito della forma scritta; Tribunale di Milano, sez. lavoro, 30 maggio 2017, in cui il messaggio WhatsApp è stato ritenuto idoneo a integrare una condotta diffamatoria e denigratoria di un lavoratore rispetto al proprio responsabile; Corte d'Appello di Roma, 23 aprile 2018, che ha ritenuto legittimo il licenziamento con messaggio WhatsApp, che, per un più generale principio di libertà della forma dei negozi giuridici, è del tutto equipollente e rispettoso delle norme del codice sull'efficacia e sulla presunzione di conoscenza degli atti unilaterali (artt. 1334-1335 c.c.). Nel caso del licenziamento è opportuno precisare che per la giurisprudenza non sussiste l'onere di adoperare formule sacramentali per l'intimazione del licenziamento, purché questo avvenga in forma scritta.

unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati»[58].
Rispetto alla firma elettronica semplice la firma elettronica avanzata si atteggia con un rapporto di *species a genus* e costituisce una firma più "forte", in quanto prevede da una parte la connessione unicamente al firmatario, idonea a identificarlo e realizzata mediante dati che il firmatario può utilizzare sotto il proprio controllo esclusivo, e dall'altra la rilevabilità di eventuali modifiche successive; non è però caratterizzata dalla presenza di un certificato qualificato, come le firme elettroniche qualificate e le firme digitali.
In relazione a tale tipologia di firma il regolamento eIDAS, le norme nazionali e le regole tecniche in materia di firme elettroniche, approvate con d.p.c.m. 22 febbraio 2013 e ancora vigenti in quanto non ancora sostituite da linee guida, prevedono esplicitamente il principio di neutralità tecnologica, che informa la normativa; il reg. (UE) n. 910/2014, infatti, elenca una serie di condizioni, senza tuttavia imporre le modalità attraverso cui garantire il soddisfacimento di dette condizioni, e gli obiettivi che devono essere soddisfatti[59]. Le disposizioni riconoscono la possibilità di realizzare, in forma libera, soluzioni di firma elettronica avanzata, senza necessità di autorizzazione preventiva e senza la previsione di vincoli tecnologici[60], ma rispettando una serie di requisiti minimi oggettivi e soggettivi[61].
Pertanto anche la firma elettronica avanzata, come quella semplice, è conforme ai principi di non discriminazione e neutralità tecnologica, dal momento che la norma dispone il soddisfacimento delle condizioni normativamente previste, ma è indifferente rispetto al tipo di tecnologia impiegata e alle modalità tecniche con cui sono soddisfatte le condizioni stesse[62].
Secondo quanto previsto dalle regole tecniche, l'utilizzabilità della firma elettronica avanzata è possibile limitatamente ai rapporti giuridici intercorrenti tra il sottoscrittore

[58] Art. 3, par. 1, n. 11) e art. 26, reg. (UE) n. 910/2014. Nella relazione illustrativa di accompagnamento allo schema di d.lgs. 235/2010 l'introduzione della firma elettronica avanzata, inserita per adeguarsi alla normativa europea (in particolare alla direttiva 1999/93/CE), trova motivazione nel fatto che, in considerazione dell'evoluzione della tecnologia, esistono una serie di soluzioni tecniche che, anche se non giungono al livello della firma digitale, sono dotate comunque di un buon livello di sicurezza e attendibilità, atte quindi a semplificare e a favorire l'uso delle nuove tecnologie.

[59] Cfr. G. Finocchiaro, *Una prima lettura del Reg. UE n. 910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari*, cit., 425 ss. Le regole tecniche, per quanto riguarda la firma avanzata, hanno introdotto una liberalizzazione che lascia agli operatori massima autonomia, rispondendo al principio di neutralità tecnologica e consentendo in tal modo l'adeguamento all'evoluzione tecnica.

[60] Fermo restando quanto disposto dall'art. 55, c. 1 (realizzazione libera e non soggetta ad autorizzazione preventiva), l'AgID elabora linee guida sulla base delle quali realizzare soluzioni di firma elettronica avanzata conformi alle regole tecniche (art. 61, c. 6, d.p.c.m. 22 febbraio 2013).

[61] Art. 55 ss., d.p.c.m. 22 febbraio 2013: le soluzioni di firma elettronica avanzata devono possedere le caratteristiche previste nell'art. 56, c. 1, per poter soddisfare i requisiti che ne conferiscono il valore giuridico e probatorio previsto dal d.lgs. 82/2005 (art. 56, c. 2).

[62] G. Finocchiaro, *Diritto di Internet*, cit., 90 ss.: la firma elettronica avanzata consiste in un processo e non in un prodotto, dal momento che devono essere soddisfatti requisiti di natura tecnologica, ma anche organizzativa.

e il soggetto che eroga soluzioni di firma elettronica avanzata al fine di utilizzarle nei rapporti intrattenuti per motivi istituzionali, societari o commerciali, realizzandole in proprio oppure avvalendosi di soluzioni realizzate da soggetti terzi che svolgono tale funzione come attività di impresa: la firma elettronica avanzata ha una sostanziale rilevanza interna nell'ambito di rapporti giuridici tra soggetti[63].

Esempi di firma elettronica avanzata sono la *one time password* e la firma biometrica o grafometrica, laddove rispettino quanto previsto dalle regole tecniche.

La firma grafometrica si basa sull'acquisizione di dati e parametri biometrici relativi al movimento compiuto dal firmatario al momento della sottoscrizione sul dispositivo digitale, quali la posizione, la velocità, il ritmo e la pressione: la firma grafometrica è qualificabile come firma elettronica avanzata, nel caso in cui ne rispetti i requisiti previsti; altrimenti è qualificabile come firma elettronica semplice[64].

Inoltre, nei rapporti con le pubbliche amministrazioni il legislatore ricorre a *fictio iuris*, conferendo il valore di firma avanzata a strumenti diversi di comunicazione e di identificazione: l'invio tramite posta elettronica certificata di cui all'art. 65, c. 1, lett. *c-bis)* del d.lgs. 82/2005, effettuato richiedendo la ricevuta completa, sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata[65] e, altresì, l'utilizzo della carta d'identità elettronica, della carta nazionale dei servizi, del documento d'identità dei pubblici dipendenti (Modello *ATe*), del passaporto elettronico e degli altri strumenti ad essi conformi sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata per i servizi e le attività di cui agli artt. 64 e 65 del d.lgs. 82/2005[66].

In merito al valore giuridico del documento informatico cui è apposta la firma elettronica avanzata e alla relativa idoneità a soddisfare il requisito della forma scritta, per gli atti di cui all'art. 1350, c. 1, nn. 1-12, c.c.[67] la norma, salvo il caso di sottoscrizione autenticata, pone la necessità della sottoscrizione con firma qualificata o digitale, a pena di nullità: sotto tale profilo queste firme mantengono dunque una più forte dignità giuridica rispetto a quella avanzata, che non è considerata sufficiente per queste tipologie di atti. Diversamente gli atti della categoria residuale di cui all'art. 1350, c. 1, n. 13), c.c. («gli altri atti specialmente indicati dalla legge»), redatti su documento informatico o formati attraverso procedimenti informatici, devono essere sottoscritti, a pena di nullità, con firma elettronica avanzata, qualificata o digitale; di conseguenza, tali atti soddisfano comunque il requisito della forma scritta anche se sottoscritti con

[63] Art. 60, d.p.c.m. 22 febbraio 2013, recante "Limiti d'uso della firma elettronica avanzata".

[64] La firma grafometrica è diffusamente impiegata nel settore bancario e assicurativo. Cfr. G. Finocchiaro, *Diritto di Internet*, cit., 91 ss.; Ead., *Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale*, cit., 498; Ead., *Firme elettroniche e firma digitale*, cit., 318 ss. In tema di biometria è intervenuto il Garante per la protezione dei dati personali con il provvedimento generale prescrittivo n. 513 del 12 novembre 2014.

[65] La ricevuta completa di avvenuta consegna è la ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale; si differenzia da quella breve, nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale, e da quella sintetica, che contiene i dati di certificazione (art. 1, c. 1, lett. *i)*, *l)* ed *m)*, d.m. 2 novembre 2005).

[66] Art. 61, c. 1 e 2, d.p.c.m. 22 febbraio 2013; cfr. TAR Campania, sez. III, 10 marzo 2015, n. 1450.

[67] Atti di costituzione e trasferimento di diritti reali immobiliari, locazioni ultranovennali, etc.

firma elettronica avanzata[68].

Sotto il profilo probatorio, il documento sottoscritto con firma elettronica avanzata, formato nel rispetto delle regole tecniche, ha l'efficacia della scrittura privata di cui all'art. 2702 c.c., ossia fa piena prova fino a querela di falso della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta[69].

In merito è interessante l'evoluzione normativa impressa al d.lgs. 82/2005 dal d.lgs. 217/2017, che ha attribuito lo stesso valore giuridico e probatorio del documento informatico cui è apposta la firma elettronica avanzata al documento formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID per mezzo di linee guida recanti regole tecniche, con modalità tali da garantire sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. Tale tipologia di sottoscrizione è stata qualificata come una *species* del *genus* firma avanzata, denominata anche firma avanzata identificata[70].

Al riguardo rilevano le linee guida contenenti le regole tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD, pubblicate il 23 aprile 2020, che prevedono il processo da seguire per la sottoscrizione basata sulle identità digitali del Sistema Pubblico per la gestione delle Identità Digitali di cittadini e imprese (denominata anche firma con SPID), che ha valore giuridico e probatorio come firma elettronica avanzata[71].

6.3. La firma elettronica qualificata e la firma digitale

Il sistema di firme elettroniche è caratterizzato dalla gradualità, dal momento che la maggiore forza si basa sulla maggiore capacità di garantire sicurezza a livello tecnologico. Per tale motivo ogni firma successiva nella scala gerarchica ha le caratteristiche della precedente, ma anche alcune caratteristiche tecniche ulteriori, idonee a conferire maggiore sicurezza: pertanto, come la firma elettronica avanzata rispetto alla firma elettronica semplice, parimenti la firma elettronica qualificata si atteggia con un rapporto di *species a genus* nei confronti della firma elettronica avanzata e la firma digitale,

[68] Art. 21, c. 2-*bis*, d.lgs. 82/2005. Al riguardo G. Finocchiaro, *Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale*, cit., 503 porta l'esempio della conclusione di contratti online in ambito bancario e dell'acquisizione del consenso in ambito sanitario. Secondo A. Gentili, *Negoziare* on line *dopo la riforma del codice dell'amministrazione digitale*, cit., 353 in tutti i casi che richiedono la firma *ad substantiam* (esclusi quelli tradizionali di disposizione di immobili), il ricorso alla firma digitale può essere surrogato dalla firma avanzata meno formalizzata e dunque di più facile utilizzo, dotata comunque di elevati standard di sicurezza, utili per la prova e per la certezza dei rapporti giuridici.

[69] Art. 20, c. 1-*bis*, d.lgs. 82/2005.

[70] Art. 20, c. 1-*bis*, d.lgs. 82/2005; tale processo è stato introdotto nel d.lgs. 82/2005 dal d.lgs. 217/2017.

[71] Le linee guida contenenti le regole tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del d.lgs. 82/2005 sono state approvate dall'AgID con determinazione n. 157/2020 del 23 marzo 2020 e pubblicate il 23 aprile 2020.

a sua volta, con rapporto di *species a genus* rispetto alla firma elettronica qualificata.
La firma elettronica qualificata è una «firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche»[72]. L'art. 25, par. 3, reg. (UE) n. 910/2014 prevede il principio di reciproco riconoscimento, secondo cui una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli Stati membri, promuovendo l'interoperabilità giuridica tra i diversi sistemi di firma, necessaria a garantire effettività e certezza nelle relazioni tra soggetti. In merito alla firma elettronica qualificata, rilevano le linee guida contenenti regole tecniche e raccomandazioni afferenti alla generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate, adottate dall'AgID con determinazione n. 121/2019 del 17 maggio 2019, rettificata con determinazione n. 147/2019 del 4 giugno 2019, e pubblicate il 20 giugno 2019.
La firma digitale, prevista in modo specifico dal nostro ordinamento giuridico, è «un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici»[73].
Nel caso della firma digitale si sceglie la crittografia a chiavi asimmetriche per garantire sicurezza: la chiave privata è utilizzata dal soggetto titolare e permette di apporre la firma digitale; la chiave pubblica è l'elemento destinato ad essere reso pubblico e permette ai soggetti terzi di verificare la firma digitale apposta. Le due chiavi sono correlate, dal momento che solo la chiave pubblica corrispondente permette di decifrare la chiave privata, e indipendenti, in considerazione del fatto che la chiave pubblica, conoscibile da chiunque, non permette di risalire alla chiave privata, conosciuta solo dal titolare. La firma digitale ricorre a una funzione di *hash* da cui si ricava l'impronta digitale o *digest* del documento che ne garantisce l'integrità[74]: tale impronta viene cifrata dal titolare con la propria chiave privata, garantendo così la provenienza del documento[75].
I formati di firma possono avere estensione .p7m (CAdES), .pdf (PAdES), .xml (XA-

[72] Art. 3, par. 1, n. 12), reg. (UE) n. 910/2014. Ai sensi dell'art. 3, par. 1, nn. 22) e 23), reg. (UE) n. 910/2014, il dispositivo per la creazione di una firma elettronica qualificata è un software o hardware configurato utilizzato per creare una firma elettronica che soddisfa i requisiti di cui all'allegato II del reg. (UE) n. 910/2014; i dispositivi cui si allude nella definizione possono essere *token* USB o *smart card*.

[73] Art. 1, c. 1, lett. *s)*, d.lgs. 82/2005: la firma digitale è prevista dal nostro ordinamento e la definizione è pertanto ancora contenuta nel CAD.

[74] Se il documento viene successivamente modificato, infatti, si produce una nuova impronta.

[75] La crittografia asimmetrica permette di garantire paternità, integrità, non ripudiabilità, autenticazione e identificazione della provenienza del documento; la sicurezza si fonda sul fatto che da un punto di vista computazionale è molto complesso (se non impossibile in termini relativi) risalire dalla chiave pubblica alla chiave privata. Cfr. M. Martoni, *Il documento informatico e le firme elettroniche nel Codice dell'amministrazione digitale*, cit., 37 ss.; G. Taddei Elmi, *Corso di Informatica giuridica*, III ed., Napoli, 2010, 289: «Un cifrario a chiave asimmetrica basa, quindi, la sua sicurezza sul concetto di complessità computazionale: non è impossibile decifrarlo, ma è ragionevolmente impossibile farlo in tempo utile. La falsificazione imporrebbe costi superiori ai vantaggi conseguibili».

dES); al riguardo si è espressa la Corte di Cassazione, sezioni unite, 27 aprile 2018, n. 10266, e, in senso conforme, Corte di Cassazione, sezioni unite, 29 novembre 2018, n. 30927, chiarendo l'equivalenza tra i diversi formati di firma secondo le norme europee[76] e nazionali, anche di carattere tecnico, e, in specifico, ritenendo che i formati di firma CAdES e PAdES sono equivalenti, pienamente validi e efficaci[77].

La firma elettronica qualificata e la firma digitale, oltre ad una maggiore garanzia a livello tecnologico, offrono maggiore sicurezza per il fatto che in entrambi i casi è prevista la presenza di un certificato qualificato[78] e, di conseguenza, emerge un significativo aspetto organizzativo di controllo, ossia l'attività di certificazione dell'identità del firmatario svolta da un soggetto terzo garante, previsto e disciplinato dalle disposizioni europee e nazionali, il prestatore di servizi fiduciari qualificato[79]. Tale soggetto per svolgere le proprie funzioni deve possedere determinati requisiti di qualità e sicurezza ed è sottoposto a obblighi e responsabilità specifiche; i soggetti che intendono fornire servizi fiduciari qualificati devono presentare domanda di qualificazione all'AgID, che in caso di accoglimento della domanda dispone l'iscrizione in un elenco pubblico, consultabile anche in via telematica[80]. Riguardo al certificato di firma, il titolare è tenuto ad utilizzare personalmente il dispositivo di firma, ad assicurarne la custodia e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri[81].

Osservate alla luce del principio di neutralità tecnologica, a differenza della firma elettronica semplice e di quella avanzata, che risultano espressioni di quei criteri, nel caso della firma elettronica qualificata e della firma digitale il principio viene meno, dal momento che si sceglie un determinato livello di sicurezza e una particolare tecnologia: si precisa la necessità che tali tipologie di firme siano basate su un certificato qualificato, che assicura l'identificazione del soggetto[82]. Lo scostamento dal principio è partico-

[76] Decisione di esecuzione UE 2015/1506 della Commissione europea dell'8 settembre 2015.

[77] Software come Digital Signature Service (DSS), DiKe, ArubaSign e Acrobat Reader DC o applicazioni online come quelle di Infocert o del Consiglio Nazionale del Notariato, soluzioni gratuite e utilizzabili con i dispositivi di firma digitale, consentono di verificare le firme digitali.

[78] Il certificato di firma elettronica è «un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona» e il certificato qualificato di firma elettronica è «un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I» (art. 3, par. 1, nn. 14) e 15), reg. UE n. 910/2014).

[79] Il prestatore di servizi fiduciari è «una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato», mentre il prestatore di servizi fiduciari qualificato è «un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato» (art. 3, par. 1, nn. 19) e 20), reg. UE n. 910/2014).

[80] I prestatori di servizi fiduciari qualificati sono sottoposti al regime giuridico disciplinato dal reg. (UE) n. 910/2014 e dall'art. 28 ss., d.lgs. 82/2005. Al riguardo rilevano, inoltre, le linee guida, adottate dall'AgID con determinazione n. 121/2019 del 17 maggio 2019, rettificata con determinazione n. 147/2019 del 4 giugno 2019, e pubblicate il 20 giugno 2019.

[81] Art. 32, c. 1, d.lgs. 82/2005, che prevede l'obbligo di custodia in riferimento al dispositivo di firma e agli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto.

[82] Cfr. G. Finocchiaro, *Firme elettroniche e firma digitale*, cit., 312 ss.: «Una delle differenze fra le varie firme è che le definizioni di firma elettronica e di firma elettronica avanzata non si riferiscono a un livello di sicurezza predeterminato o a una tecnologia precisa. Sono "neutre" [...]. Invece, le definizioni di firma elettronica qualificata e digitale sono collegate a livelli di sicurezza predeterminati e ad una tecnologia

larmente evidente nel caso della firma digitale, *species* del *genus* della firma qualificata, dove, oltre al livello di sicurezza predefinito del certificato qualificato, si sceglie e si esplicita normativamente la crittografia asimmetrica quale tecnologia necessaria per raggiungere gli obiettivi di sicurezza e affidabilità[83].

La natura non tecnologicamente neutra di tali firme si traduce anche negli effetti giuridici che sono esplicitamente disciplinati dal legislatore.

In merito al valore giuridico, la sottoscrizione del documento informatico con firma elettronica qualificata o firma digitale equivale alla sottoscrizione autografa e il documento informatico soddisfa il requisito della forma scritta a pena di nullità (*ad substantiam*) ai sensi dell'art. 1350 c.c., anche nei casi di cui ai numeri da 1 a 12 del comma 1[84]; il legislatore in tal caso determina *ex ante* l'equivalenza tra tali tipologie di firma e la sottoscrizione autografa.

L'efficacia probatoria del documento sottoscritto con firma elettronica qualificata o firma digitale, formato nel rispetto delle regole tecniche, è quella della scrittura privata ai sensi dell'art. 2702 c.c., ossia fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione ovvero se questa è legalmente considerata come riconosciuta. In merito, le disposizioni pongono una presunzione legale di utilizzo, che invece non riguarda la firma elettronica avanzata: l'utilizzo del dispositivo di firma elettronica qualificata o digitale «si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria»[85]. Ciò comporta l'inversione dell'onere probatorio a carico del titolare del dispositivo di firma, che deve fornire la prova di non averlo utilizzato; di conseguenza, non si tratta di disconoscimento in senso tecnico (la specifica firma digitale si collega in modo matematico al titolare), ma di disconoscimento in senso lato, dal momento che non si disconosce la firma, ma la sua apposizione[86]. L'inversione dell'onere probatorio determina in tali casi l'efficacia probatoria rafforzata rispetto al documento cartaceo[87].

Al momento della sottoscrizione il certificato qualificato non deve risultare scaduto di validità, revocato o sospeso, dal momento che l'apposizione a un documento informatico di una firma digitale o di altro tipo di firma qualificata basata su certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione, salvo che

predefinita» (314).

83 Cfr. G. Finocchiaro, *Diritto di Internet*, cit., 89; M. Martoni, *Il documento informatico e le firme elettroniche nel Codice dell'amministrazione digitale*, cit., 44 ss.

84 Atti di costituzione e trasferimento di diritti reali immobiliari, locazioni ultranovennali, etc.; art. 21, c. 2-*bis*, d.lgs. 82/2005. Ai sensi dell'art. 25, reg. (UE) n. 910/2014 una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa. Cfr. G. Finocchiaro, *Diritto di Internet*, cit., 96, la quale al riguardo richiama la sentenza della Corte d'Appello di Venezia, sezione II, 13 giugno 2018, che per la costituzione di un vincolo di natura reale ha ritenuto l'email, quale firma elettronica, non idonea a soddisfare il requisito della forma scritta *ad substantiam*.

85 Art. 20, c. 1-*ter*, d.lgs. 82/2005.

86 Al riguardo G. Finocchiaro, *Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale*, cit., 501 ss. parla di un nuovo tipo di disconoscimento che ha ad oggetto l'utilizzo del dispositivo di firma (e non la firma digitale o la scrittura), passando così da un criterio di "paternità" a un criterio di "responsabilità".

87 G. Finocchiaro, *Diritto di Internet*, cit., 95.

lo stato di sospensione sia stato annullato[88].

Al riguardo emerge la rilevanza dell'aspetto temporale evidenziato anche all'inizio dell'analisi, ossia l'individuazione temporale e la data certa: «le firme elettroniche qualificate e digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato»[89].

Costituiscono validazione temporale elettronica[90] la marca temporale, ossia il «riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo»[91] e i riferimenti temporali ottenuti per mezzo di: segnatura di protocollo; procedura di conservazione dei documenti in conformità alle norme vigenti ad opera di un pubblico ufficiale o di una pubblica amministrazione; utilizzo della posta elettronica certificata; utilizzo della marcatura postale elettronica ai sensi della Convenzione postale universale[92]. Riguardo all'aspetto temporale dei documenti, data e ora di formazione del documento informatico sono opponibili a terzi se apposte in conformità alle linee guida[93].

Il d.p.c.m. 22 febbraio 2013 prevede, inoltre, due particolari procedure informatiche di firma elettronica qualificata o digitale, che ne condividono effetti giuridici e valore probatorio: la firma remota e la firma automatica[94].

Accanto alle quattro tipologie di firma elettronica esaminate, si parla di firma autenticata nel caso in cui la firma elettronica o qualsiasi altro tipo di firma elettronica avanzata sia riconosciuta ai sensi dell'art. 2703 c.c., ossia sia autenticata da notaio o da altro pubblico ufficiale a ciò autorizzato[95]: l'autenticazione, anche mediante l'acquisizione digitale della sottoscrizione autografa o di qualsiasi altro tipo di firma elettronica avanzata, consiste nell'attestazione da parte del pubblico ufficiale del fatto che la sottoscrizione è stata apposta in sua presenza dal titolare, previo accertamento della

[88] Art. 24, c. 3 e 4-*bis*, d.lgs. 82/2005: «La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate».

[89] Art. 62, d.p.c.m. 22 febbraio 2013.

[90] Ai sensi dell'art. 3, par. 1, n. 33), reg. (UE) n. 910/2014 costituisce validazione temporale elettronica «un insieme di dati in forma elettronica che associano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento»: può essere semplice o qualificata (se rispetta quanto previsto dall'art. 42, reg. UE n. 910/2014) con effetti giuridici diversi.

[91] Art. 1, c. 1, lett. *i)*, d.p.c.m. 22 febbraio 2013.

[92] Art. 41, c. 4, d.p.c.m. 22 febbraio 2013.

[93] Art. 20, c. 1-*bis*, d.lgs. 82/2005.

[94] La firma remota, che viene generata a distanza, è una «particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse» e la firma automatica, particolarmente indicata per la sottoscrizione massiva di documenti informatici, è una «particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo»; l'HSM è un «insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche» (art. 1, c. 1, lett. *p)*, *q)* e *r)*, d.p.c.m. 22 febbraio 2013). Cfr. G. Finocchiaro, *Diritto di Internet*, cit., 91 ss.

[95] Art. 25, c. 1, d.lgs. 82/2005.

sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento non è in contrasto con l'ordinamento giuridico[96]. Tale tipologia di firma ha quindi maggiore valore probatorio, in quanto viene attestata non solo la certezza dell'identità, ma anche l'utilizzo della firma da parte del legittimo titolare e l'effettiva volontà.

Infine, va menzionato l'atto pubblico informatico redatto dal notaio, regolato dal d.lgs. 2 luglio 2010, n. 110[97], che equivale e produce i medesimi effetti del corrispondente cartaceo, in quanto anche in tal caso interviene il pubblico ufficiale che fornisce piena certezza[98].

Pertanto, nell'ordinamento emerge un sistema graduale di firme elettroniche, capaci di attribuire diverso valore giuridico e probatorio al documento cui sono apposte, in conformità alla differente capacità tecnologica di garantire affidabilità e conseguente certezza del diritto.

7. Aspetti critici e riflessioni conclusive

L'analisi relativa al valore giuridico e probatorio delle firme elettroniche mostra i mutamenti profondi che caratterizzano il passaggio dalla firma autografa alla firma elettronica, che non si limitano soltanto all'utilizzo di un diverso mezzo di sottoscrizione. Firma autografa e firma elettronica differiscono, in primo luogo, per le modalità di apposizione, dal momento che la firma elettronica è il risultato di una procedura informatica e non di un gesto umano. La firma elettronica, infatti, si basa sulla tecnica, ontologicamente impersonale, e non sulla grafia, strettamente legata alla persona, aspetto che incide anche sul criterio di imputazione e sulla natura del disconoscimento, che nel caso della firma elettronica qualificata e digitale si distingue da quello tradizionale basato sulla perizia calligrafica, per atteggiarsi più propriamente come disconoscimento in senso lato, dal momento che non si disconosce la firma, ma la sua apposizione: al riguardo si pone la connessa problematica relativa all'individuazione di quale tipo

[96] Art. 25, c. 2, d.lgs. 82/2005, modificato dal d.lgs. 235/2010, che ha allargato l'area delle firme autenticabili (in precedenza, l'autenticazione poteva avere ad oggetto solo firme qualificate o digitali); ai sensi dell'art. 25, c. 3, d.lgs. 82/2005 il pubblico ufficiale appone la firma digitale o qualificata con l'efficacia prevista dall'art. 24, c. 2: «l'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente». La modifica è coerente con l'art. 52-*bis*, legge notarile 89/1913, novellata dal d.lgs. 110/2010.

[97] Il d.lgs. 110/2010 ha novellato la legge notarile 89/1913. Ai sensi dell'art. 21, c. 2-*ter*, d.lgs. 82/2005, fatto salvo quanto previsto dal d.lgs. 110/2010, ogni altro atto pubblico redatto su documento informatico è sottoscritto dal pubblico ufficiale a pena di nullità con firma qualificata o digitale. Le parti, i fidefacenti, l'interprete e i testimoni sottoscrivono personalmente l'atto, in presenza del pubblico ufficiale, con firma avanzata, qualificata o digitale ovvero con firma autografa acquisita digitalmente e allegata agli atti.

[98] Cfr. C. Sgobbo, *Il valore probatorio dell'e-mail (nota a Trib. Prato, 15 aprile 2011)*, in *Il Corriere del merito*, 8-9, 2011, 804; A. Gentili, *Negoziare* on line *dopo la riforma del codice dell'amministrazione digitale*, cit., 354: «Strumenti come la firma non avanzata per gli atti che si potrebbero compiere *verbis*, la firma avanzata per gli atti scritti più usuali (movimenti sui conti correnti, operazioni di investimento, rapporti assicurativi, atti dei consumatori con i professionisti, o informazioni dei professionisti ai consumatori, e simili), e la firma digitale per gli atti scritti più solenni (eventualmente autenticata o apposta all'atto pubblico) soddisfano tutte le esigenze».

di prova permetta questo disconoscimento, aspetto su cui soccorre l'art. 32 del d.lgs. 82/2005, fornendo criteri di riferimento al riguardo[99].

Un altro profilo significativo di differenza tra firma autografa e firma elettronica attiene ai soggetti coinvolti nel processo di firma: nelle tipologie di firma elettronica più affidabili, qualificata e digitale, che si basano sul livello di sicurezza predeterminato dal legislatore e individuato nel certificato qualificato, nel processo di firma non è coinvolto soltanto il firmatario, come avviene nella firma autografa, ma anche un soggetto terzo che si pone quale garante, emergendo la sua cruciale funzione organizzativa di controllo. Questo aspetto scaturisce dalla profonda diversità ontologica tra firma autografa e firma elettronica e dal fatto che nella seconda rileva una procedura informatica che determina anche l'esigenza di soggetti qualificati a presidiarla.

Tra gli aspetti differenziali non può essere sottaciuto un profilo afferente alle norme che regolano le due tipologie di firma, dal momento che nel caso delle firme elettroniche la tecnologia è regolata da un complesso eterogeneo di fonti, anche di natura tecnica. Di conseguenza, particolare valore nella realizzazione concreta delle stesse rivestono non solo le norme di rango primario, tese a individuare i principi di riferimento, ma altresì le regole tecniche e gli standard contenuti in atti di *soft law*, quali le linee guida dell'AgID, di cui il Consiglio di Stato ha chiarito il carattere di vincolatività: regole tecniche e standard sono deputati a dare applicazione ai principi giuridici, forieri di criteri di bilanciamento tra interessi, ma, in ragione della diversa genesi rispetto alle norme strettamente intese, è opportuno precisare che su tale tipologia di regole possono incidere concretamente eventuali portatori di interessi[100].

Evidenziare i molteplici aspetti di differenza tra firma autografa e firma elettronica permette di comprendere anche il difficile adattamento alla mutata dimensione digitale delle norme civilistiche, adeguate alla realtà analogica, la conseguente difficile regolazione della tecnologia, peraltro in continua evoluzione, e le problematiche che possono insorgere concretamente.

Al riguardo è necessario osservare che il *framework* giuridico è in evoluzione, dal momento che la Commissione europea ha presentato la proposta di regolamento «che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea», COM(2021) 281 *final* del 3 giugno 2021, con l'obiettivo di migliorarne l'efficacia ed estenderne i benefici, promuovendo identità digitali sicure e affidabili. La proposta di regolamento si concentra sull'identità digitale europea e non incide significativamente sul sistema di firme elettroniche, ma, dal momento che riguarda le identità digitali, indirettamente riguarda anche un processo di firma, giacché il legislatore ha previsto nel nostro ordinamento la sottoscrizione basata sulle identità digitali del sistema SPID, attribuendole il valore di firma elettronica avanzata. Pertanto le modifiche al sistema delle identità digitali, in cui deve inserirsi

[99] «Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma» (art. 32, c. 1, d.lgs. 82/2005). Cfr. G. Finocchiaro, *Diritto di Internet*, cit., 86 ss.; G. Pascuzzi (a cura di), *Il diritto dell'era digitale*, cit., 128 ss.

[100] Cfr. G. Finocchiaro, *Diritto di Internet*, cit., 86 ss.; G. Pascuzzi (a cura di), *Il diritto dell'era digitale*, cit., 128 ss.

necessariamente il sistema italiano SPID, determinano un potenziale impatto su questa specifica tipologia di firma.

Inoltre, al fine di rispondere alle dinamiche dei mercati e agli sviluppi tecnologici, la proposta di regolamento espande l'attuale elenco di servizi fiduciari, aggiungendo tra i nuovi servizi fiduciari qualificati la gestione di dispositivi per la creazione di firme e sigilli elettronici a distanza, che, secondo quanto espresso esplicitamente, sarebbe idonea ad apportare notevoli vantaggi in termini di sicurezza, uniformità, certezza del diritto e scelta dei consumatori, legati tanto alla certificazione dei dispositivi per la creazione di firme qualificate quanto ai requisiti che devono essere soddisfatti dai prestatori di servizi fiduciari qualificati che gestiscono tali dispositivi. A tal fine la proposta di regolamento prevede un nuovo articolo 29-*bis* nel regolamento (UE) n. 910/2014, che definisce i requisiti relativi ai servizi qualificati per la gestione di dispositivi per la creazione di una firma elettronica a distanza.

Nella consapevolezza di una costante evoluzione normativa in materia, il *framework* giuridico europeo e nazionale in tema di firme elettroniche si caratterizza per i principi di neutralità tecnologica e non discriminazione, criteri che discendono strettamente dall'oggetto di regolazione, la tecnologia, e che più ampiamente permeano la normativa in materia di amministrazione digitale e innovazione tecnologica. Nello specifico contesto delle firme elettroniche tali principi si atteggiano diversamente a seconda delle tipologie, dal momento che nelle firme più forti la tecnologia è predefinita e il livello di sicurezza è predeterminato *ex ante* dal legislatore, rendendo di conseguenza le firme qualificata e digitale tecnologicamente non neutre.

La normativa di riferimento, infatti, seppur permeata da questi principi, è tesa a garantire quale obiettivo ultimo adeguata certezza ai rapporti tra soggetti e, a tal fine, ad assicurare validità ai documenti e alle attività giuridiche compiute nella dimensione digitale.

La normativa persegue la certezza del diritto, ma nell'applicazione della stessa emergono criticità, con il conseguente rischio che si verifichi uno scollamento tra il quadro normativo (e gli obiettivi cui è teso) e l'applicazione delle regole alle fattispecie concrete.

L'analisi del sistema di firme elettroniche mostra questo aspetto nell'applicazione della disciplina giuridica ad alcuni strumenti, peraltro di uso particolarmente diffuso nelle relazioni interpersonali. È il caso di email, SMS e WhatsApp, che come esaminato, sono inquadrati in modo diverso nella giurisprudenza e cui, di conseguenza, è attribuito anche un diverso valore giuridico e probatorio, complice la disposizione che in caso di documento informatico non sottoscritto o accompagnato da firma elettronica rimette alla discrezionalità del giudice la valutazione concreta; nei fatti ciò si è tradotto in oscillazioni e sentenze di tenore diverso, pur richiamando le stesse norme di riferimento.

Se la firma elettronica semplice è sicuramente manifestazione piena del principio di neutralità tecnologica e non discriminazione, proprio per il fatto che non sono predeterminati dal legislatore il livello di sicurezza richiesto e la tecnologia da impiegare, è opportuno rilevare che ciò comporta concretamente come contrappeso il rischio di venire meno al fine stesso di tutta la disciplina, ossia la certezza nelle relazioni in-

terpersonali, dal momento che nell'applicazione concreta emergono legittimamente interpretazioni diverse da parte dei giudici, a seconda delle caratteristiche del caso concreto. Questo non permette, pertanto, agli utilizzatori della firma elettronica semplice di conoscere l'effettivo valore giuridico e probatorio nel momento del suo impiego. In considerazione del diffuso utilizzo degli strumenti indicati (email, SMS, WhatsApp) la diversa attribuzione di valore probatorio può incidere sull'effettiva tutela dei diritti in contesti giuridici diversi di particolare impatto sulla vita sociale ed economica della persona (relazioni contrattuali, rapporti di lavoro, condotte illegittime, quali quelle diffamatorie, etc.).

Sotto tale profilo i principi di neutralità tecnologica e non discriminazione, criteri cardine della disciplina, mostrano profili affini nel caso della firma elettronica avanzata, che parimenti intrepreta pienamente i principi europei di riferimento. È il caso della firma grafometrica, che è qualificabile come firma elettronica avanzata, laddove rispetti le condizioni e i requisiti previsti, altrimenti avrà il valore della firma elettronica semplice. Non è sufficiente si tratti di una firma grafometrica perché abbia il valore giuridico e probatorio della firma elettronica avanzata, ma è necessario che le condizioni previste, anche di tenore organizzativo, siano rispettate.

A questi profili critici deve essere sommata qualche scelta da parte del legislatore nazionale, che al fine di semplificare i rapporti, in particolare tra amministrazioni e cittadini, favorendo questi ultimi in quanto soggetti deboli del rapporto, ha previsto alcune *fictio iuris*, determinando sovrapposizioni tra firme elettroniche e strumenti che nascono con *ratio* diverse, quali i mezzi di comunicazione telematica e gli strumenti di identificazione. Al riguardo, preme ricordare, infatti, che l'invio tramite posta elettronica certificata di cui all'art. 65, c. 1, lett. *c-bis)* del d.lgs. 82/2005, effettuato richiedendo la ricevuta completa, sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata e, altresì, l'utilizzo della carta d'identità elettronica, della carta nazionale dei servizi, del documento d'identità dei pubblici dipendenti (Modello *ATe*), del passaporto elettronico e degli altri strumenti ad essi conformi sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata per i servizi e le attività di cui agli artt. 64 e 65 del d.lgs. 82/2005[101].

Operazione simile viene compiuta con lo strumento di identificazione garantito dal Sistema Pubblico per la gestione delle Identità Digitali di cittadini e imprese (SPID), che consente l'identificazione informatica del soggetto e dà forma al concetto di identità digitale nella sua accezione "ristretta" di carattere oggettivo, che si collega a un valore di carattere pubblicistico. Il legislatore, infatti, attribuisce lo stesso valore giuridico e probatorio della firma elettronica avanzata al documento formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID per mezzo di linee guida recanti regole tecniche, con modalità tali da garantire sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore; tale tipologia di sottoscrizione è stata qualificata come una *species* del *genus* firma avanzata[102]. Al riguardo opportunamente l'ordinamento ha previsto uno strumento di *soft law*, teso a regolare il processo speci-

[101] Art. 61, c. 1 e 2, d.p.c.m. 22 febbraio 2013.

[102] Art. 20, c. 1-*bis*, d.lgs. 82/2005.

fico e indicare le condizioni necessarie: si tratta delle linee guida contenenti le regole tecniche per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD, pubblicate il 23 aprile 2020. Il ricorso alle linee guida permette di intercettare l'obiettivo di sicurezza e certezza che la disciplina in materia si pone, dettagliando il processo da seguire per la sottoscrizione basata sulle identità digitali del sistema SPID.

Evidentemente minori problematiche applicative relative alla qualificazione e al valore giuridico e probatorio sollevano le firme "forti" e tecnologicamente non neutre, quali la firma elettronica qualificata e la firma digitale, anche se trattandosi di tecnologie predefinite, governate da regole e standard tecnici, possono porsi problemi concreti nella gestione e nella verifica delle stesse. Dal momento che si tratta di una procedura informatica, la verifica, infatti, è possibile soltanto in modo indiretto con un *medium* ossia un software, che darà la "sentenza" circa la validità o meno della firma stessa. Al riguardo, però, non possono essere esclusi eventuali errori e non mancano a livello pratico applicazioni che decretano come non valide sottoscrizioni basate su certificati emessi in conformità al regolamento eIDAS da soggetti europei, a causa di errori dovuti a scostamenti di bit[103]. Inoltre, sugli stessi formati di firma e sulla loro validità ed efficacia, si è dovuta esprimere la Corte di Cassazione, chiarendo l'equivalenza tra i diversi formati di firma secondo le norme europee e nazionali, anche di carattere tecnico, e, in specifico, tra i formati CAdES e PAdES[104].

Pertanto, tra firma semplice e firma avanzata, da una parte, e firma qualificata e firma digitale, dall'altra, emergono problematiche di ordine diverso, ma parimenti presenti nel momento dell'applicazione del quadro regolatorio europeo e nazionale alle eterogenee fattispecie concrete.

Accanto agli esaminati profili di criticità che nell'applicazione concreta le diverse tipologie di firma elettronica possono esprimere, alcuni aspetti problematici derivano dalla natura ontologica stessa delle firme, ossia dal fatto che si tratta di tecnologie: da tale profilo consegue che, in primo luogo, le firme elettroniche sono governate necessariamente anche da regole tecniche e, in secondo luogo, sono caratterizzate da una costante e rapida evoluzione.

Sotto il primo profilo, la necessità che i principi giuridici espressi nelle norme di rango primario debbano trovare applicazione nelle regole tecniche può generare criticità in caso di mancata o ritardata emanazione delle stesse, rendendo "zoppo" l'impianto normativo di riferimento e determinando la possibile mancata o inadeguata applicazione delle disposizioni in attesa dell'emanazione delle regole di attuazione. Peraltro, proprio al fine di scongiurare questo problema, che più ampiamente affligge le norme secondarie e le regole tecniche di attuazione delle norme in materia di amministrazione digitale e innovazione, a livello nazionale le regole tecniche hanno subito negli ultimi anni un processo di deregolamentazione, passando dai d.p.c.m. del passato alle attuali linee guida di AgID, connotate da una rapida produzione, maggiormente flessibili e adatte agli scopi, di cui il Consiglio di Stato ha comunque esplicitato la valenza *erga omnes* e il carattere di vincolatività.

---

[103] Così G. Manca, *Firma informatica oggi e domani: stato dell'arte e prospettive di sviluppo*, in *agendadigitale.eu*, 6 dicembre 2021.

[104] Cass. civ., sez. un., 27 aprile 2018, n. 10266, e Cass. civ., sez. un., 29 novembre 2018, n. 30927.

Nonostante questo, in materia di firme elettroniche al momento sono state pubblicate solo le linee guida contenenti le regole tecniche e le raccomandazioni afferenti alla generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate (il 20 giugno 2019) e le linee guida per la sottoscrizione elettronica di documenti ai sensi dell'art. 20 del CAD (il 23 aprile 2020); di conseguenza, nelle more della produzione delle regole tecniche mancanti, per quanto non disciplinato restano ancora vigenti le regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali di cui al d.p.c.m. 22 febbraio 2013. Tali regole tecniche però sono state prodotte prima dell'emanazione del regolamento eIDAS e rischiano di non essere più conformi alle disposizioni europee, che peraltro sono contenute in un regolamento e, di conseguenza, sono direttamente applicabili.

Sotto il secondo profilo, l'evoluzione tecnologica incide nella creazione di strumenti giuridici diversi dal passato con cui le parti regolano i propri rapporti. È quanto accaduto a livello contrattuale, dove si assiste al cambiamento di paradigma dal documento e dal contratto analogici a quelli informatici, in cui mutano forma e modalità di conclusione e, talvolta, di esecuzione, affidate a codici e software.

Al riguardo, le problematiche si atteggiano diversamente a seconda delle diverse ipotesi che si configurano nel momento della formazione e del perfezionamento del contratto, che possono avvenire con scambio di comunicazioni telematiche oppure con accesso a un sito web. Nel caso di perfezionamento a distanza "via Internet", servendosi di un mezzo di trasmissione telematica emergeranno differenze relative alla validità giuridica e probatoria, a seconda dell'utilizzo o meno delle firme elettroniche e in considerazione del fatto che sia richiesta o meno una forma scritta per la conclusione; di conseguenza troverà applicazione *de plano* il sistema di firme elettroniche previste dall'ordinamento con le problematiche esaminate nel caso di utilizzo di strumenti come email, SMS e WhatsApp.

Diverso è invece il caso della conclusione del contratto "in Internet", tramite accesso a un sito web. Nel caso di perfezionamento del contratto telematico per mezzo dell'accesso al sito quale "vetrina virtuale" e con una contrattazione per adesione, secondo il modello estremamente diffuso nel commercio elettronico (basta pensare a piattaforme di *e-commerce* come Amazon), l'accettazione espressa avviene attraverso la pressione del cosiddetto tasto negoziale virtuale, il *point and click*, cui viene assegnata la manifestazione di volontà, oppure per mezzo del pagamento attraverso la digitazione dei numeri della carta di credito. Il tasto negoziale virtuale può essere ritenuto firma elettronica semplice e l'idoneità impegnativa in tal caso deriva dal fatto che l'espressione ha tipicità sociale, capace di comportare consapevolezza del passaggio dalle fasi di informazione e valutazione a quella dell'impegnatività giuridica; al riguardo può essere applicato l'art. 1326, comma 4, c.c.: «qualora il proponente richieda per l'accettazione una forma determinata, l'accettazione non ha effetto se è data in forma diversa»[105].

Tale fattispecie è rilevante per l'analisi in oggetto, dal momento che nella gerarchia delle firme elettroniche il *point and click* può essere interpretato come mera firma elet-

[105] Cfr. V. Cuffaro, *Profili di tutela del consumatore nei contratti online*, in G. Finocchiaro – F. Delfini (a cura di), *Diritto dell'informatica*, Torino, 2014, 381 ss.

tronica semplice con il relativo valore giuridico e probatorio "incerto", rimesso al giudizio, dal momento che a livello tecnico si tratta della firma più debole dell'ordinamento. Nell'era digitale, tali negozi, cui possono essere assimilati i contratti conclusi tramite *app*[106], sono estremamente diffusi: in tal caso soccorrono una serie di ulteriori considerazioni fondate sulle norme civilistiche, che permettono di attribuire validità a uno strumento che si è imposto nel mercato digitale per la semplicità di utilizzo e per la capacità di consentire l'agevole circolazione di beni tra i soggetti. Tale modalità di conclusione del contratto, che risponde agli obiettivi perseguiti dai principi di neutralità e non discriminazione, mostra con evidenza come l'evoluzione tecnologica incida sui rapporti negoziali e li plasmi, portando l'interprete a dover "leggere" la realtà concreta con le lenti dell'impianto normativo di riferimento.

Sotto tale profilo l'evoluzione tecnologica non solo incide sugli strumenti giuridici, ma genera tecnologie emergenti che possono essere impiegate nelle relazioni negoziali e sono foriere di problematiche inedite, per le quali può essere particolarmente complessa l'applicazione del quadro normativo, sorto per affrontare fattispecie diverse. In particolare l'evoluzione ha generato tecnologie che incidono proprio sulle transazioni, quali la *blockchain*[107], e possono essere impiegate nei negozi giuridici: a livello contrattuale si assiste pertanto negli ultimi anni all'ulteriore sviluppo dei contratti digitali verso gli *smart contracts*, dove muta il linguaggio di riferimento, si compie una piena automazione e la tecnologia è capace di sostituirsi all'uomo.

Nello *smart contract*, nel momento in cui sono soddisfatte le condizioni contrattuali tradotte dal codice informatico nel linguaggio macchina, si attivano automaticamente gli effetti conseguenti con le caratteristiche tipiche della *blockchain*, in particolare l'immutabilità e l'irreversibilità: gli effetti contrattuali si eseguono automaticamente al verificarsi delle condizioni predeterminate dalle parti e descritte sotto forma di codice informatico secondo la logica "*if this then that*"; si determina così un meccanismo di *self enforcement* delle regole.

Evidentemente già dalla descrizione dello strumento giuridico emerge la difficile applicazione allo stesso delle disposizioni europee e nazionali relative al sistema di firme elettroniche, risultando problematica l'attribuzione del documento informatico costi-

[106] Le *app* (applicazioni) possono essere native (sviluppate per un determinato sistema operativo come iOS e Android), web (una sorta di collegamento all'applicazione che non è fisicamente installata sul dispositivo, ma accessibile tramite *browser*) e ibride (usate spesso per testare un'applicazione prima di lanciarla come nativa); generalmente si trovano nei cosiddetti *app store*, negozi virtuali attraverso cui vengono rese disponibili al pubblico (es. Google Play); cfr. A.M. Gambino – A. Stazi – D. Mula, *Diritto dell'informatica e della comunicazione*, III ed., Torino, 2019, 176 ss.

[107] La *blockchain* è una *species* del *genus* delle *distributed ledger technologies* (DLT), ossia tecnologie di registro distribuito e disintermediato *peer-to-peer*, in cui le voci del database sono replicate in una serie di nodi e la regolazione avviene mediante meccanismi di consenso condiviso; le DLT si distinguono dalle architetture centralizzate *client-server*, basate invece sul controllo di un'autorità di gestione. In specifico la *blockchain* consiste in una "catena di blocchi", ciascuno contenente una o più transazioni: i dati, inseriti per mezzo di crittografia asimmetrica, sono allocati in blocchi, accompagnati da *hash* e *timestamp*, concatenati tra loro attraverso il richiamo dell'*hash* del blocco precedente in quello successivo. Ogni nuovo blocco è validato da alcuni nodi (*miners*) per mezzo della risoluzione di un problema matematico complesso, che vale una ricompensa; le transazioni sono validate con il consenso della maggioranza degli utenti. La *blockchain*, in modo immutabile, conserva la memoria storica delle transazioni e, in modo distribuito e paritetico, garantisce a ciascun partecipante una copia di ciascuna operazione: in tal modo sono garantite sicurezza e resistenza rispetto a potenziali attacchi.

tuito dallo *smart contract* al soggetto che lo ha creato[108] ed essendo difficile conciliare la *lex cryptographia* degli *smart contracts* con le regole poste dal diritto positivo[109]; tali difficoltà sono aggravate dalle disposizioni del nostro ordinamento riguardo al fenomeno, che generano problematiche applicative.

Il nostro ordinamento definisce lo "*smart contract*" nel comma 2 dell'art. 8-*ter* del d.l. 135/2018, convertito dalla legge 12/2019, come «un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse», con una qualificazione normativa che oscilla tra software e documento informatico; il legislatore precisa che lo *smart contract* soddisfa il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'AgID con linee guida.

Pertanto, ai fini della riconducibilità del documento informatico al soggetto, lo *smart contract* può essere ascritto al processo di cui all'art. 20, comma 1-*bis*, del d.lgs. 82/2005, ossia può qualificarsi come firma elettronica avanzata identificata, con il relativo valore giuridico e probatorio[110]. Ma questa interpretazione si attaglia alle *blockchains permissioned*, dove i partecipanti sono previamente identificati, mentre può non essere adeguata alle *blockchains permissionless*[111]. In tal caso, laddove, a causa dell'assenza dei requisiti normativi necessari, non possa essere riconosciuto il valore di firma elettronica avanzata, il valore giuridico e probatorio saranno rimessi alla libera valutazione del giudice, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità, ai sensi dell'art. 20, comma 1-*bis*, d.lgs. 82/2005[112]. Di conseguenza, la norma italiana solleva tale significativo aspetto critico afferente all'idoneità ad assolvere il requisito della forma scritta, che può mutare a seconda della tipologia di *blockchain* impiegata e che, anche in tal caso, scaturisce strettamente dalle caratteristiche tecniche e organizzative concrete: il valore giuridico e l'efficacia probatoria sono diversi in conformità alla differente capacità di garantire sicurezza e affidabilità circa l'identità dei soggetti e l'integrità dei dati. L'analisi delle firme elettroniche mostra, pertanto, alcune criticità nell'applicazione a strumenti di diffuso utilizzo, come email, SMS, WhatsApp, nella conclusione del contratto con accesso a un sito web, e, altresì, al cospetto di tecnologie emergenti

[108] Cfr. M. Giuliano, *La blockchain e gli* smart contracts *nell'innovazione del diritto nel terzo millennio*, in *Il diritto dell'informazione e dell'informatica*, 6, 2018, 989 ss.

[109] Cfr. G. Lemme, *Gli* smart contracts *e le tre leggi della robotica*, in *Analisi Giuridica dell'Economia*, 1, 2019, 148, che evidenzia come «il processo di divaricazione piena tra *civil law* (ma tutto sommato anche *common law*) e *lex cryptographia* si stia oramai ineluttabilmente compiendo».

[110] Cfr. G. Finocchiaro, *Il contratto nell'era dell'intelligenza artificiale*, in *Rivista trimestrale di diritto e procedura civile*, 2, 2018, 441 ss.; C. Bomprezzi, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, in *Diritto, mercato, tecnologia*, 2019, 4 ss.

[111] Le *blockchains permissionless* o *unpermissioned* o pubbliche, aperte e liberamente accessibili da chiunque senza autorizzazione, si distinguono dalle *blockchains permissioned* o private, che sono chiuse e non accessibili pubblicamente, dal momento che le autorizzazioni sono gestite da un'autorità centrale e, pertanto, prevedono una forma di *governance*. Inoltre esistono le *blockchains* ibride, dette altresì consorzi, parzialmente decentrate, nelle quali esiste un controllo sul meccanismo di consenso da parte di alcuni nodi preselezionati, che hanno maggiore influenza degli altri.

[112] Cfr. C. Bomprezzi, *Commento in materia di Blockchain e Smart contract alla luce del nuovo Decreto Semplificazioni*, cit., 5; F. Sarzana Di S. Ippolito – M. Nicotra, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, 2018, 51 ss.

come *blockchain* e *smart contract*, che evolvono la concezione del contratto, ponendo problematiche nuove. In queste fattispecie il quadro normativo sconta un difficile adattamento e rischia di non garantire quella certezza nelle relazioni negoziali, cui la normativa è diretta. Sotto tale profilo gli stessi principi di neutralità tecnologica e non discriminazione, che plasmano la disciplina, e gli obiettivi a cui sono diretti (concorrenza, autonomia, effettività e adeguamento all'evoluzione tecnologica) devono essere bilanciati con l'esigenza di sicurezza, affidabilità e certezza, che ha determinato l'esistenza stessa di firme tecnologicamente non neutre, come quella qualificata e quella digitale, non a caso anche le più forti.

Sicuramente nel futuro sarà necessario garantire un quadro "completo" delle fonti in materia con l'emanazione di linee guida, la cui mancanza determina problemi attuativi e che possono essere la sede per affrontare problematiche poste concretamente da strumenti specifici e tecnologie determinate, che caratterizzano le concrete attività giuridiche nella dimensione digitale.

Come nel caso di altre tecnologie, anche per le firme elettroniche il diritto è chiamato al difficile compito di trovare un complesso equilibrio con la tecnologia, al fine di rispettarne l'evoluzione e le opportunità che consente, ma allo stesso tempo assicurare sicurezza nei rapporti tra esseri umani. Del resto il diritto è una scienza che nasce per conferire certezza alle relazioni, riuscendo a tutelare gli uomini e le loro attività: la regolazione giuridica deve riuscire ad assolvere questo compito nella dimensione digitale come in quella analogica.