DE IUSTITIA

Rivista scientifica Marzo 2024

DIRITTO CIVILE ISSN 2974-7562

L'EFFICACIA PROBATORIA DELLA POSTA ELETTRONICA

di **Alessandra PRANDI** *

ABSTRACT

Le sentenze in commento hanno ad oggetto controversie nascenti dalla mancata ricezione di un messaggio di posta elettronica: nel caso del Tribunale di Milano si tratta di una e-mail ordinaria tramite la quale la convenuta informava parte attrice sulle disposizioni della merce; nel caso della Corte d'Appello di Napoli, invece, la mancata ricezione è riferita aduna PEC contente una notifica di un decreto ingiuntivo.

Analizzando i criteri su cui si fonda la paternità di una e-mail ordinaria e quali sono gli oneri e gli obblighi gravanti sui titolari di una casella PEC e sui loro gestori, il presente contributo intende esaminare e poi confrontare i riflessi di questi due metodi di comunicazioni in ambito probatorio.

SOMMARIO

1. DUE RECENTI RISCONTRI GIURISPRUDENZIALI

Con la sentenza n. 8547/2022 il Tribunale di Milano ha condannato la società convenuta KHRYSOS S.R.O. al risarcimento del danno per la mancata fornitura di taluni prodotti ad alta rotazione a favore della società attrice VALUE MED S.R.L. Nello specifico, le due società avevano stabilito che il venditore avrebbe stipulato un'assicurazione sui prodotti in cessione, che l'acquirente avrebbe versato un acconto pari alla metà del prezzo totale pattuito per la fornitura e che, infine, il venditore avrebbe messo a disposizione i beni per il ritiro presso la sede logistica del venditore. Nonostante il pagamento dell'acconto, l'attrice lamentava che la merce non fosse mai giunta alla destinazione concordata né, dunque, fosse mai stata messa a sua disposizione. La convenuta sosteneva, per contro, di aver informato tempestivamente via *e-mail* la controparte della mancata disponibilità della merce a causa di un sinistro stradale, indipendente dalla sua volontà, e che in un secondo momento la compagnia assicurativa le aveva comunicato che i prodotti erano stati recuperati e resi disponibili per la società acquirente. La convenuta conseguentemente invitava via *e-mail* parte attrice al ritiro. Quest'ultima contestava di aver ricevuto tale comunicazione e disconosceva l'autenticità e la conformità delle *e-mail* riportate dalla convenuta nella comparsa di costituzione e risposta al documento oggetto di discussione. Inoltre, negava la fedeltà di dette comunicazioni ai fatti accaduti, motivando tale eccezione sulla base di una pluralità di incongruenze in ordine alla data indicata, all'impaginazione e alla mancanza degli indirizzi per esteso dei destinatari, nonché in relazione al testo di una medesima *e-mail*, prodotta da entrambe le parti, ma con contenuti non perfettamente coincidenti. Considerata l'univocità degli elementi sulla base dei quali era stato operato il disconoscimento, il Giudice ha negato efficacia probatoria alle *e-mail* prodotte da parte convenuta e, di riflesso, ha escluso che fosse stata fornita la prova della conoscenza di parte attrice circa la disponibilità della merce.

Nel caso deciso dalla sentenza della Corte di Appello di Napoli n. 2827/2023, la contestazione si fondava, invece, sulla trasmissione di una comunicazione di posta elettronica certificata (di seguito anche «PEC»), contenente la notifica di un decreto ingiuntivo e i relativi allegati, inviata dal difensore della appellante D.M.R. MEDICAL S.R.L. alla appellata CITIEFFE S.R.L. In particolare, quest'ultima non ha negato la ricezione presso la propria casella PEC, ma ha fondato la difesa sul fatto che il messaggio fosse stato considerato (dall'incaricato della società alla visione della casella) come portatore di *virus* informatici; e che, nel

* Dottoranda Università degli Studi di Brescia.

periodo tra la ricezione e la scadenza dei termini dell'opposizione, e più precisamente per tre giorni, il sistema del gestore Aruba avesse presentato malfunzionamenti. In questo caso, la Corte d'Appello di Napoli ha reputato inverosimile che il messaggio di posta elettronica certificata potesse essere stato considerato portatore di *virus* informatici, dal momento che il mittente era facilmente riscontrabile nei pubblici elenchi e l'oggetto riportava la dicitura corretta prevista per legge per le notifiche. Il Giudice, inoltre, non ha considerato rilevanti i malfunzionamenti del sistema; e ha comunque valutato negligente la condotta di Citieffe S.r.l., che proprio in ragione di tali malfunzionamenti avrebbe dovuto contattare il mittente o attivare un altro dispositivo abilitato e connesso alla rete.

2. LA "PATERNITÀ" DELLA E-MAIL ORDINARIA E LA "SOTTOSCRIZIONE ELETTRONICA"

Nella decisione del Giudice di Milano sono stati presentati diversi elementi ad evidenziare la differenza fra le due *e-mail* prodotte in giudizio, uno dei quali è l'assenza per esteso dell'indirizzo di posta elettronica e, quindi, la mancanza di riconoscimento della paternità dello specifico messaggio elettronico. L'incertezza sull'identificazione dell'utente ha avuto, e ha tutt'ora, rilevanti ripercussioni[1]: infatti, la sola presenza del nome della persona - giuridica o fisica - di riferimento, senza l'indicazione dell'indirizzo *e-mail*, non garantisce alcuna certezza in merito al soggetto che ha inviato o ha ricevuto il messaggio, potendo anche essere utilizzati pseudonimi e/o nomi falsi[2]. Per questo motivo, il Regolamento EidaS[3] distingue, all'art. 3, comma 1, rispettivamente ai punti n. 1 e n. 5, l'"identificazione elettronica" dall'"autenticazione elettronica". Più precisamente, il Regolamento definisce la prima un «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'autenticazione elettronica il «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». I due concetti sono strettamente collegati e regolano diverse fasi del processo che accompagna la trasmissione di un messaggio di posta elettronica: l'accesso all'*account*, la stesura del testo contenuto nella *e-mail* e, infine, il suo invio.

Talvolta la giurisprudenza ha considerato sufficiente, ai fini della sottoscrizione digitale, una *e-mail* spedita da un indirizzo di posta elettronica riferibile ad una società[4]. In questo caso[5], è stato

[1] ORLANDI, *Il falso digitale*, Milano, 2003, 46: «Qualsiasi testo implica la distanza dal soggetto formante ed il problema dell'imputazione; esso non è più il soggetto che parla o che scrive, ma il prodotto di quel parlare o di quello scrivere, rispetto al quale l'originario autore è lontano ed assente. Il problema dell'imputazione nasce con il distacco del dichiarato dal dichiarante, e con l'autonoma ed indipendente circolazione del testo».

[2] Cfr., sul punto, FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, 2018, 445-446, che sottolinea la delicatezza del tema affrontato anche per i contratti c.d. telematici. Evidente, peraltro, che, se viene utilizzato uno pseudonimo, la certezza delle parti viene a mancare: «i dati pseudonimizzati rimangono dati personali. La pseudonimizzazione, infatti, non esclude la possibilità di re-identificazione dell'interessato. Essa è piuttosto una misura di sicurezza che non modifica i presupposti di legittimità del trattamento dei dati personali. [...]. Il dato anonimo, invece, a cui non si applica la normativa in materia di protezione dei dati personali, è il dato che in origine o a séguito di trattamento non può essere associato a un interessato identificato o identificabile».

[3] Il Regolamento eIDAS (denominato anche Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014) disciplina le linee guida in tema di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

[4] Trib. Milano, 18 ottobre 2016, n. 11402, in *Resp. civ. e prev.*, 2017, IV, 1340, consultabile anche su https://www.fiif.it/wp-content/uploads/2016/12/sentenza-consolandi-eidas.pdf.

[5] La sentenza del Tribunale di Milano del 2016 fa riferimento all'opposizione a decreto ingiuntivo per il pagamento di fatture per compensi di un contratto di collaborazione in materia di grafica e informatica concluso via *e-mail*: «parte attrice eccepisce che si tratti di un documento non firmato. In realtà si tratta di posta elettronica spedita dall'indirizzo della società attrice e, quindi, poiché in forza dell'articolo 46 del regolamento europeo eIDAS (n. 910 del 2014) "a un documento elettronico non sono negati gli effetti giuridici e la ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica", l'argomento della carenza di sottoscrizione, connaturato ai documenti informatici, non può essere considerato». Inoltre, l'art. 25 del Regolamento eIDAS enuncia il principio di non discriminazione della firma elettronica rispetto a quella materiale: «a una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti delle firme

riconosciuto pieno valore probatorio alle *e-mail* prive di firma elettronica, sul presupposto che un documento informatico o una firma elettronica producono effetti sul piano processuale e sono pienamente ammissibili come prova nei procedimenti giudiziali per il solo motivo della loro forma elettronica, richiamando gli artt. 25 e 46 del Regolamento EidaS. Pertanto, se l'*e-mail* c.d. ordinaria è riconducibile a una determinata società, ciò sarebbe sufficiente ai fini della firma elettronica (art. 3 del Regolamento EidaS). Seguendo il percorso logico del Giudice milanese del 2016, dunque, il motivo della decisione risiede anche nel fatto che la *e-mail* è pienamente riferibile alla società di riferimento ed è, quindi, considerata sottoscritta da colui che possiede le credenziali necessarie per accedere all'*account* societario.

Occorre, dunque, interrogarsi se l'inserimento delle credenziali per accedere al sistema di posta elettronica sia designabile quale firma elettronica semplice[6] e se ciò consenta, quindi, di ritenere qualsiasi *e-mail* inviata da uno specifico indirizzo di posta elettronica sempre e automaticamente sottoscritta dal titolare dello stesso *account*.

In un primo momento[7], si è ritenuto che l'*e-mail* ordinaria dovesse considerarsi un documento munito di firma elettronica c.d. semplice, perché per inviarla è necessario inserire le proprie credenziali nel sistema di posta elettronica, ricorrendo, così, ad un metodo di autenticazione; ma si escludeva che ciò fosse sufficiente a rendere la *e-mail* sottoscritta in maniera avanzata[8], qualificata[9] o digitale[10]. Infatti, la firma elettronica, nella sua prima formulazione, si considerava quale insieme di dati in forma elettronica «allegati oppure connessi tramite associazione logica ad altri dati elettronici utilizzati come metodo di autenticazione informatica». In questa impostazione, l'*e-mail* era considerata un

elettroniche qualificate». In conclusione, si può affermare che «la spedizione [di una *e-mail*] da un indirizzo [di posta elettronica] riferibile ad una certa società [...] deve essere ritenuto firma elettronica».

[6] La firma elettronica semplice (FES) si ricava, da un lato, dall'art. 3, comma 1, n. 10, Regolamento eIDAS, il quale prevede una descrizione generale di "firma elettronica" considerandola semplicemente come una serie di «dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare»; e, dall'altro, dagli artt. 3, comma 1, n. 11 e 26 Regolamento eIDAS, i quali si occupano delle "firme elettroniche avanzate". Quella presa in considerazione è, infatti, una categoria residuale: in cui confluiscono tutti i sistemi di sottoscrizione informatica capaci di individuare l'autore, ma che non soddisfano i requisiti previsti *ex lege* perché si possa definire firma elettronica avanzata.

[7] Cfr. ARNÒ - LISTA, *La firma digitale nell'ordinamento italiano e comunitario*, in *Riv. dir. civ.*, 2000, II, 781 ss.; CERDONIO CHIAROMONTE, *Il valore dell'email nel quadro della disciplina dei documenti informatici*, in *Riv. dir. civ.*, 2021, 449 ss.; COLAROCCO, COGODE, *L'efficacia probatoria della mail non certificata,* in *Dir. Internet*, 2020, 373 ss.; CORSINI e ORBINI MICHELUCCI, *Sostituire il documento cartaceo con il documento informatico, firmarlo e trasmetterlo in rete*, in *Dir. Internet*, 2006, III, 311-312; PANI, *Il valore di prova scritta di una e-mail: la giustizia inizia a porsi al passo coi tempi*, nota a Trib. Cuneo, 15 dicembre 2003, n. 848, in *Giur. mer.*, 2005, 560 ss.; RICCI, *L'efficacia probatoria dell'e-mail non sottoscritta*, in *Riv. trim. dir. proc. civ.*, 2021, 629 ss.; SCARPA, *Riflessioni sull'e-mail come possibile prova scritta ai fini dell'emissione del decreto ingiuntivo*, in *Nuove leggi civ. comm.*, 2001, I, 3 ss. In giurisprudenza cfr. *ex pluribus* Trib. Cuneo, 15 dicembre 2003, n. 848, in *Giur. it.*, 2005, I, 1024-1025, e in *Giur. mer.*, 2005, 560 ss.

[8] La firma elettronica avanzata (FEA) è un sistema di sottoscrizione che assicura maggiore tutela al firmatario rispetto alla firma elettronica semplice in virtù dei diversi requisiti imposti dal Regolamento (UE) 910/2014 che consentono un'univoca riconducibilità del documento informatico al firmatario stesso. L'art. 26 del Regolamento eIDAS prevede, infatti, che la firma elettronica sia: a) connessa unicamente al firmatario; b) idonea a identificare il firmatario; c) creata mediante dati che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo e d) collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica degli stessi.

[9] La firma elettronica qualificata (FEQ) è definita dall'art. 3, comma 1, n. 12 del Regolamento eIDAS quale «firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato per firme elettroniche». Ne possiamo dedurre che costituisce una sottocategoria della firma elettronica avanzata, ovvero oltre ad avere le principali caratteristiche di quest'ultima, presenta ulteriori requisiti che la rendono ancora più sicura: viene generata da un apposito dispositivo e si basa su un certificato elettronico qualificato.

[10] La firma digitale è prevista esclusivamente dal nostro ordinamento quale *species* della FEQ. Ai sensi dell'art. 1, comma 1, lett. s), CAD, essa è considerata come «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». Il tratto distintivo della firma digitale è appunto l'utilizzo simultaneo di queste due chiavi crittografiche: una privata e una pubblica, di cui la prima nota solo al titolare dell'utenza e la seconda a chiunque vi abbia interesse. Tra le due chiavi esiste un nesso «tale che il documento cifrato dal firmatario con la chiave privata può essere decifrato solo avvalendosi della corrispondente chiave pubblica»; tuttavia ciò non significa che, avendo a disposizione la chiave pubblica, si possa risalire automaticamente alla privata e viceversa (chiavi crittografiche c.d. "asimmetriche").

documento informatico munito di sottoscrizione semplice[11]. Peraltro, a seguito dell'entrata in vigore del d.lgs. 4 settembre 2006, n. 159, la definizione di "firma elettronica" è stata modificata e fondata esclusivamente sul concetto di «metodo di identificazione informatica». Nonostante tale modifica alteri, evidentemente, il significato di "firma elettronica" fino a quel momento sostenuto, una parte della giurisprudenza[12] ha continuato a sostenere che l'inserimento delle credenziali di accesso fosse sufficiente per configurare una firma elettronica semplice e, di conseguenza, che l'*e-mail* ordinaria potesse essere ritenuta a tutti gli effetti un documento munito di sottoscrizione elettronica semplice[13]. Seguendo questa linea interpretativa, e al contrario di quanto affermato nella sentenza di Milano in commento, l'attribuzione della paternità dell'*e-mail* sarebbe collegata alla digitazione di *username* e *password*.

Per effetto dell'ulteriore modifica della definizione di "firma elettronica" apportata al Regolamento eIDAS[14], attualmente in vigore, pare difficile sostenere che il semplice inserimento delle credenziali di accesso possa considerarsi una firma elettronica semplice. I dati elettronici devono infatti essere inseriti dall'autore del documento «per firmare» e, quindi, per «assumersi la paternità della dichiarazione contenuta nel documento»[15]. In tal senso anche la Suprema Corte[16] considera l'*e-mail* ordinaria un documento privo di qualsiasi firma elettronica[17].

Infatti, nonostante si possa certamente ritenere che tale digitazione configuri un insieme di dati elettronici e un metodo di autenticazione o di identificazione informatica, ciò che manca è l'elemento essenziale che consente di definire una firma come elettronica e, cioè, la *connessione logica* di tali elementi (elettronici) con la singola *e-mail* scritta e inviata a seguito dell'accesso all'*account* da parte del titolare, mediante l'inserimento - una sola volta - delle proprie credenziali. Siffatta *connessione logica* esisterebbe unicamente se venisse richiesto l'inserimento al momento dell'invio di ciascun messaggio, e non solo in una fase anteriore alla sua stesura. Si ritiene[18], quindi, che l'inserimento delle credenziali abbia la mera funzione di autenticazione per ottenere dall'*Internet Service Provider* il servizio di ricezione, lettura e invio della posta elettronica e non, anche, la funzione di assumersi la paternità del singolo messaggio inviato[19].

[11] Cfr., ad es., JORI, *L'efficacia probatoria dell'e-mail*, nota a Trib. Cuneo, 15 dicembre 2003, n. 848, in *Giur. it.*, 2005, I, 1024-1025.

[12] Cfr., ad es., Trib. Prato, 15 aprile 2011, cit., con commento di SGOBBO, *Il valore probatorio dell'e-mail*, Trib. Termini Imerese, 22 febbraio 2015, cit. Si veda anche Trib. Firenze, 14 marzo 2018, n. 780, in *Redazione Giuffrè*, 2018, per la quale «[d]eve in ogni caso ritenersi correttamente eseguita la denuncia di sinistro trasmessa al *broker* via *e-mail*, così come previsto nella polizza, sia che si aderisca all'orientamento secondo il quale la *e-mail* costituisce un semplice documento informatico privo di firma il cui valore probatorio è comunque da rinvenirsi nell'art. 2712 c.c., sia che si aderisca all'orientamento secondo il quale la *e-mail* è da considerare, a tutti gli effetti, un documento informatico sottoscritto con firma elettronica semplice, come tale liberamente valutabile dal giudice in ordine all'idoneità della medesima a soddisfare il requisito della forma scritta, e per ciò che concerne il suo valore probatorio, ai sensi degli artt. 20, comma 1-*bis* e 21, comma 1, d.lgs. n. 82 del 2005».

[13] Cfr., ad es., Trib. Prato, 15 aprile 2011, cit. *Contra*, Trib. Roma, 27 maggio 2010, in *Dir. informatica*, 2011.

[14] [Art. 3, comma 1, n. 10, Regolamento (UE) 910/2014]: «dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare».

[15] CERDONIO CHIAROMONTE, *Il valore dell'email*, cit., 432.

[16] Cass., 14 maggio 2018, n. 11606, in *Giust. Civ.*, 2018, 523.

[17] Cfr., sul punto, Cass., 6 febbraio 2019, n. 3540, in *Resp. civ. e prev.*, 2019, II, 653; Cass., 17 luglio 2019, n. 19155, in *Guida dir.*, 2019, 33, 104.

[18] Cfr. BARBARO, *Il valore giuridico probatorio delle mail, il dibattito dottrinale e giurisprudenziale in materia e la sentenza in epigrafe. Una voce fuori dal coro?,* nota a Trib. Roma, 27 maggio 2010, in *Dejure*, 529.

[19] CERDONIO CHIAROMONTE, *Il valore dell'email*, cit., 430-431. Sul punto, crf. BARBARO, *Il valore giuridico probatorio delle mail*, cit., 529; BUONOMO, *Il magistrato: scritto e trascritto, ma non sottoscritto*, in *Interlex*, 29 gennaio 2004, disponibile su https://www.interlex.it/docdigit/buonomo10.htm; CAMMARATA - MACCARONE, *Un messaggio e-mail non è prova scritta*, in *Interlex*, 29 gennaio 2004, disponibile su https://www.interlex.it/docdigit/provascrita.htm; DI BENEDETTO, *Scrittura privata e documento informatico. Riconoscimento disconoscimento e verificazione*, Milano, 2009, 328; FARINA, *Riflessioni sul valore legale dell'e-mail a seguito della pronuncia di alcuni decreti ingiuntivi basati esclusivamente sulla produzione di una e-mail*, in *Rass. dir. vic.*, 2005, III, 615; JORI, *L'efficacia probatoria dell'e-mail*, cit., 1024 ss.; Trib. Bari, 20 gennaio 2004; Trib. Mondovì, 7 giugno 2004, n. 375; Trib. Lucca, 17 luglio 2004; Giud. Pace Pesaro, 2 novembre 2004, n. 598, tutte in *Giur. it.*, 2005, V, 1024 ss.; RICCHIUTO, *Gli effetti probatori del documento informatico*, in *Interlex*, 5 febbraio 2004; ROGNETTA, *Decreti ingiuntivi basati su e-mail: la configurabilità della firma elettronica ai fini della prova scritta*, in *Dir. Internet*, 2005, 37. In particolare, anche Trib. Roma, 27 maggio 2010, cit.: la decisione ha stabilito che le *e-mail* c.d. ordinarie possano considerarsi come documenti

Devono essere del resto valutati alcuni aspetti tecnici: *in primis*, non esiste alcuna certezza in merito all'autenticità del testo di una *e-mail* c.d. ordinaria, essendo esso facilmente modificabile[20]; inoltre, l'inserimento delle credenziali è spesso memorizzato da *browser* e *software* per la gestione della posta elettronica, in modo che l'utente medio non sempre è in grado di disattivarli (o preferisce non farlo). Ne segue, come nel caso deciso dal Tribunale di Milano, che va negata la possibilità di considerare il messaggio di posta elettronica un documento informatico munito di firma elettronica semplice, poiché non vi è alcun collegamento logico tra credenziali di accesso e documento oggetto di invio e ricezione[21]. Una fattispecie, questa, che produce effetti probatori solo nell'ambito delle riproduzioni meccaniche e informatiche *ex* art. 2712 c.c. (come vedremo nel paragrafo n.4).

3. LA POSTA ELETTRONICA CERTIFICATA COME METODO DI NOTIFICA. ONERI E OBBLIGHI GRAVANATI SUI TITOLARI DI UNA CASELLA PEC E SUI LORO GESTORI

Nella decisione della Corte d'Appello di Napoli oggetto di contestazione è la visualizzazione di un messaggio di posta elettronica certificata da parte della Società Citieffe S.r.l. Al fine di comprendere meglio le ragioni della decisione, pare tuttavia necessaria una premessa sul tema.

La posta elettronica certificata riveste oggi un ruolo centrale nell'ambito del processo civile telematico e in tutte le comunicazioni che intercorrono tra privati, tra pubbliche amministrazioni e tra privati e pubbliche amministrazioni. Inoltre, con il DM 3 aprile 2013, n. 48[22], l'utilizzo della PEC è divenuto mezzo per l'esecuzione delle notifiche nel processo civile telematico. L'introduzione della PEC, la regolamentazione delle modalità di funzionamento della stessa, l'efficacia probatoria e i soggetti gestori del servizio di posta elettronica certificata sono stati però disciplinati da distinti interventi normativi disorganici[23].

La posta elettronica certificata è stata originariamente disciplinata dall'art. 27, comma 8, l. 16 gennaio 2003, n. 3[24], il quale prevede anche l'introduzione di uno o più regolamenti volti a estendere l'utilizzo della PEC sia nei rapporti tra pubbliche amministrazioni sia nei rapporti tra pubbliche amministrazioni e privati. Tale previsione legislativa contiene la prima definizione di posta elettronica certificata, come un «sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici»[25] e stabilisce, inoltre, che il messaggio di posta elettronica certificata è esso stesso un «documento informatico composto dal testo del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati»[26].

Fino all'entrata in vigore delle Regole tecniche di cui al d.m. 21 febbraio 2001, n. 44, la PEC non veniva sempre utilizzata come mezzo di notificazione nel processo civile telematico[27].

informatici dotati di sottoscrizione semplice. Secondo tale orientamento, difatti, l'inserimento delle credenziali costituisce una modalità di identificazione non sufficiente, tuttavia, nell'ipotesi di invio di un messaggio di posta elettronica, in quanto l'elemento che viene meno è proprio quella *connessione logica* richiesta tra singola *e-mail* e l'accesso all'*account*, ossia l'inserimento delle credenziali al momento dell'apertura della propria posta elettronica.

[20] La modificabilità della *e-mail* risiede nel fatto che, quando si "risponde" a una *e-mail* o la si "inoltra", quest'ultima può essere modificata in calce alla *e-mail* che si intende scrivere.

[21] Cfr. BARBARO, *Il valore giuridico probatorio delle mail*, cit., 530.

[22] Il d.m. 3 aprile 2013, n. 48 è entrato in vigore nel maggio 2013.

[23] Cfr. TAFFARI, *Il processo telematico. Analisi ragionata delle disposizioni legislative e regolamentari*, Roma 2015, 78 ss.

[24] PORCELLI, *La posta elettronica certificata*, in *Il processo telematico nel sistema del diritto processuale civile*, a cura di Ruffini, Milano 2019, 99. «Le origini della PEC sono state peraltro da alcuni fatte risalire già alla l. 15 marzo 1997, n. 59, secondo la quale il sistema di posta elettronica certificata si estrinsecava nella trasmissione di un messaggio tra due caselle di posta elettronica, di cui venga data al mittente la segnalazione [...] del giorno e dell'ora dell'avvenuta o mancata consegna del messaggio».

[25] Art. 1, comma 2, lett. *g*, d.P.R. 11 febbraio 2005, n. 68.

[26] Art. 1, comma 2, lett. *f*, d.P.R. 11 febbraio 2005, n. 68.

[27] PORCELLI, *La posta elettronica certificata*, cit., 97 s. Fino all'entrata in vigore del d.m. 21 febbraio 2001, n. 44 si utilizzava una specifica posta elettronica certificata che veniva generata dal punto di accesso del Portale dei servizi telematici al momento dell'iscrizione al Portale medesimo (c.d. CPECPT). Il CPECPT era adibito a ricevere solo comunicazioni provenienti da uguali caselle di posta e il suo unico impiego era per lo svolgimento di attività processuale.

Successivamente, l'art. 4, comma 2, d.l. 29 dicembre 2009, n. 193 ha esteso l'utilizzo della PEC anche al processo penale e sancito tale impiego per tutte le comunicazioni e notificazioni telematiche nel processo civile. Infatti, il D.L. n. 179/2012[28] all'art. 16 stabilisce che «le comunicazioni e notificazioni di cancelleria nel settore civile sono effettuate esclusivamente per via telematica». Affinché un messaggio di posta elettronica certificata sia «valido agli effetti di legge»[29] è necessario verificare l'autenticità della casella PEC del mittente, l'integrità della trasmissione, l'autenticità e integrità del contenuto e, infine, la data e l'ora dell'invio della comunicazione, siccome risultano dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna[30]. In realtà, nel caso esaminato dalla Corte d'Appello di Napoli, non sono in discussione tali elementi[31], bensì gli oneri e gli obblighi gravanti sui titolari di una casella PEC e sui loro gestori. In particolare, secondo la Corte, l'addetto alla consultazione della casella PEC della Società Citieffe S.r.l. avrebbe potuto intuire che non si trattava di un messaggio di posta elettronica certificata "indesiderata" per mezzo di alcuni elementi quali l'indirizzo PEC del mittente e la dicitura obbligatoria per la notifica telematica degli atti giudiziari e dei relativi allegati.

Il legislatore è intervenuto a più riprese al fine di regolamentare gli indici nazionali degli indirizzi di posta elettronica certificata, inserendo l'obbligo per le imprese e per i professionisti di munirsi di una propria casella PEC[32]. Difatti, gli indirizzi virtuali risultanti da pubblici elenchi, individuati dalla legge ed enumerati in maniera tassativa all'art. 16-*ter*, d.l. n. 179/2012, sono indispensabili per le notificazioni e comunicazioni a mezzo PEC. Ai fini della validità della notifica in formato digitale, non basta l'invio del messaggio a una qualsiasi casella di posta elettronica certificata del destinatario (il quale potrebbe disporre di più di un indirizzo PEC) conosciuta dal notificante, occorrendo anche che tale indirizzo risulti in pubblici elenchi[33]. Prima dell'entrata in vigore del d.l. n. 179/2912, infatti, «gli elenchi degli indirizzi elettronici che potevano essere consultati anche dai privati [...] erano l'elenco degli indirizzi di posta certificata delle pubbliche amministrazioni [...] e gli elenchi degli indirizzi PEC contenuti nel Registro generale degli indirizzi elettronici (ReGIndE)»[34]. Oltre a quest'ultimo[35], vengono oggi considerati pubblici elenchi anche l'elenco dei domicili digitali delle imprese e dei professionisti (c.d. INI-PEC)[36], il registro delle

[28] D.L. 18 ottobre 2012, n. 179.

[29] Art. 4 d.P.R. 11 febbraio 2005, n. 68.

[30] La ricevuta di accettazione e quella di avvenuta consegna sono delle "notifiche" inviate automaticamente dal proprio sistema PEC al momento della consegna del messaggio di posta elettronica certificata presso un altro indirizzo PEC. Attraverso tali strumenti è possibile ricavare l'istante di avvenuta consegna, utile e valido in sede processuale.

[31] Infatti, la Società Citieffe S.r.l. ha espressamente dichiarato di aver ricevuto la PEC inviata da D.M.R. Medical S.r.l. e i relativi allegati.

[32] BRUNELLI, *Contributo allo studio della notificazione telematica*, in *Riv. trim. dir. proc. civ.*, 2019, 112 s. Conseguentemente, il d.P.R. n. 68/2005 ha demandato all'allora Ministro per l'innovazione e le tecnologie l'incarico di emanare un decreto che stabilisca delle regole tecniche per la formazione, trasmissione e validazione della posta elettronica certificata. Più precisamente, gli elementi applicativi del d.P.R. summenzionato sono: *i*) il decreto n. 19818 del Ministero per l'innovazione e le tecnologie del 2 novembre 2005 che disciplina le "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata" che descrivono i requisiti tecnico-funzionali che le piattaforme utilizzate dai gestori per erogare il servizio devono rispettare e *ii*) la circolare CNIPA n. 49 del 24 novembre 2005, successivamente sostituita con la circolare n. 56 del 21 maggio 2009, che «definisce le modalità con cui i soggetti [...] che intendono esercitare l'attività di gestori di posta elettronica certificata, devono presentare le relative domande di iscrizione all'elenco pubblico dei gestori e i requisiti tecnico-organizzativi che essi devono possedere». In argomento, v. anche RIEM, *Il processo civile telematico: come depositare gli atti*, Sarcangelo di Romagna 2014, 202; SALA, *E-mail, PEC, CPECPT, caratteristiche e differenze*, in *Imm. e proprietà* 2009, 718 ss.; SALA, *Il processo telematico del 2010*, in *Imm. e proprietà* 2009, 177 s.

[33] Art. 3-*bis*, l. n. 53 del 21 gennaio 1994.

[34] BRUNELLI, *Gli indirizzi virtuali qualificati per le notificazioni telematiche secondo la Cassazione*, in *Riv. trim. dir. e proc. civ.*, 2019, 1044. In particolare, il riassetto di tali elenchi pubblici è il risultato di una nuova configurazione di elenchi già esistenti, dell'istituzione di nuovi registri e della soppressione di vecchi indici.

[35] Il Registro Generale degli Indirizzi Elettronici (ReGIndE) è gestito dal Ministero della Giustizia e disciplinato dall'art. 7 d.m. n. 44/2011 e dalle specifiche tecniche di cui agli artt. 7, 8 e 9, provvedimento DGSIA 16 aprile 2014. Si tratta di una sorta di *database* costituito dai dati identificativi e dagli indirizzi PEC dei difensori delle parti private, degli avvocati iscritti in elenchi speciali, degli avvocati e procuratori dello Stato, degli altri difensori appartenenti ad enti pubblici, dei professionisti non iscritti ad alcun albo. Tale indice viene alimentato dagli elenchi creati dagli ordini professionali e contenenti i dati identificativi e gli indirizzi PEC degli iscritti.

[36] L'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INI-PEC), cui all'art. 6-bis CAD, è un elenco realizzato partendo dai registri di indirizzi PEC formati presso il registro delle imprese e gli ordini o collegi professionali. Tale

imprese[37], l'elenco degli indirizzi PEC delle Pubbliche Amministrazioni (c.d. Registro PA)[38] e l'Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel registro delle imprese[39].

Nel caso di specie, gravava sul destinatario (o sul gestore) l'onere di verificare se l'indirizzo PEC del mittente provenisse da uno degli elenchi sopra menzionati, consultabili facilmente tramite i portali resi disponibili sui rispettivi siti *internet*[40].

Inoltre, ai titolari di una casella PEC viene richiesto di impiegare un *software* idoneo a verificare l'assenza di *virus* informatici per ogni messaggio in arrivo e in partenza. Tale sistema consiste in un *software antispam* capace di intercettare la trasmissione di messaggi indesiderati. Contestualmente viene richiesto anche l'utilizzo di un servizio che rilevi in automatico l'imminente saturazione della casella di PEC, al fine di assicurare la ricezione di tutti i messaggi PEC inviati[41]. Il legislatore non prevede però alcuna conseguenza in ordine al mancato rispetto di tali adempimenti, motivo per il quale si ritiene che i titolari di un indirizzo PEC siano i soli responsabili della gestione della propria utenza. In altri termini, questi hanno l'onere di consultare periodicamente la casella di posta e di verificare la presenza di eventuali messaggi, anche qualora siano stati catalogati dal proprio sistema alla stregua di "posta indesiderata". In sede processuale non sarà dunque possibile eccepire la mancata apertura della casella di posta indesiderata per giustificare l'ignoranza del messaggio inviato correttamente dal mittente[42]. Il problema risiede nel fatto che l'omissione di *software* idonei a prevenire l'intrusione di *virus* e a segnalare la saturazione della casella di posta elettronica non evita il perfezionamento della trasmissione di un messaggio a mezzo PEC, atteso che detta trasmissione si perfeziona con la consegna del messaggio nella casella PEC del destinatario, indipendentemente dall'avvenuta lettura. Tale ultimo aspetto ha evidenti conseguenze processuali sul decorso dei termini, i quali maturano indipendentemente dalla mancata lettura del relativo messaggio PEC.

L'omessa lettura non costituisce infatti giusta causa di rimessione nei termini, salvo che la parte dimostri che questa non è dipesa da fatto proprio, bensì da caso fortuito o da forza maggiore[43]. In altre parole, una volta che il mittente riceve il messaggio automatico dalla casella d'utenza, sia di ricevuta di accettazione sia di ricevuta di avvenuta consegna,

registro è, dunque, alimentato da informazioni già contenute in altri elenchi, che tuttavia non sono accessibili pubblicamente. L'art. 6-*quinquies*, comma 1, CAD stabilisce che «la consultazione *on-line* degli elenchi di cui agli articoli 6-*bis*, 6-*ter* e 6-*quater* è consentita a chiunque senza necessità di autenticazione», di conseguenza si può affermare che la funzione dell'INI-PEC è quella di rendere pubblico l'accesso agli indirizzi PEC dei professionisti e delle imprese, dando contestualmente la possibilità di utilizzare tale strumento per effettuare notificazioni nei processi.

[37] Il Registro delle imprese, inserito tra i pubblici elenchi dall'art. 66, comma 5, d.lgs. n. 217/2017 e che può essere utilizzato a partire dal 27 gennaio 2018, data in cui è entrato in vigore tale decreto legislativo, è un registro formato e gestito presso l'ufficio del registro delle imprese e che si alimenta grazie all'obbligo che grava in capo alle imprese, sia individuali che collettive, di iscrivere il proprio indirizzo PEC presso lo stesso registro.

[38] Il Registro degli indirizzi PEC delle Pubbliche Amministrazioni dedicato alle notificazioni telematiche, disciplinato all'art. 16, comma 12, d.l. n. 179/2012, è gestito presso il Ministero della Giustizia e consultabile solo dagli uffici giudiziari, dagli uffici notificazioni, esecuzioni e protesti e dagli avvocati.

[39] L'Indice nazionale dei domicili digitali delle persone fisiche e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel registro delle imprese, di cui all'art. 6-*quater* CAD, è stato istituito dall'art. 9, comma 2, d.lgs. n. 217/2017, ma la sua realizzazione e gestione è affidata alle Linee Guida AgID e confluisce proprio nell'Anagrafe nazionale della popolazione residente (ANPR). Infine, secondo l'art. 3-*bis*, comma 1-*bis* CAD, chiunque ha la facoltà di eleggere il proprio domicilio digitale, di iscriverlo nel summenzionato elenco e di richiederne la cancellazione e, quindi, anche i professionisti iscritti in albi ed elenchi possono eleggere domicilio, fermo restando che il loro domicilio digitale è l'indirizzo PEC inserito nell'INI-PEC.

[40] Nel caso di specie, il gestore della casella di posta elettronica certificata della Società Citieffe S.r.l. avrebbe potuto vedere che la PEC dell'Avvocato era presente nel registro ReGIndE, nonché nell'Indice Nazionale degli Indirizzi PEC (INI-PEC).

[41] DELLA COSTANZA - GARGANO, *Guida pratica al processo telematico*, Milano 2013 e RUGGERI, *L'avvocato e il deposito telematico degli atti civili*, Piacenza 2015.

[42] Cass. sez. lav. 2 luglio 2014 n. 15070.

[43] In giurisprudenza cfr. Cass. 2 luglio 2014, n. 15070, cit. In dottrina cfr. PORCELLI, *Le comunicazioni e le notificazioni*, in *Il processo telematico nel sistema del diritto processuale civile*, a cura di *Ruffini*, Milano 2019, 363, secondo cui da tale operazione logica «si delinea la questione relativa alla prova della tempestività dell'esercizio di poteri processuali per il compimento dei quali la legge fissa un termine che decorre dalla comunicazione (o dalla notificazione) di cancelleria, essendo in proposito necessario individuare le modalità con le quali fornire la prova del perfezionamento della comunicazione».

può presumere fin da subito l'avvenuta lettura del messaggio[44].

Da ultimo, grava sul soggetto titolare della casella di PEC l'onore di assicurare il corretto funzionamento della rete telefonica o telematica, in quanto il destinatario di un messaggio PEC non può far valere la mancata lettura del messaggio per inconvenienti relativi alla rete, come, invece, ha cercato di fare la Società Citieffe S.r.l[45].

4. I RIFLESSI PROBATORI: L'E-MAIL ORDINARIA

Preso atto che la tesi prevalente esclude che l'inserimento delle credenziali di accesso all'*account* di posta elettronica sia equiparabile a una firma elettronica semplice e che l'*e-mail* sia da ritenersi automaticamente documento informatico munito di tale firma elettronica semplice[46], è da rilevare che il dibattito si articola ulteriormente su due posizioni alternative. Alcuni ritengono che alle *e-mail* prive di firma elettronica debba attribuirsi l'efficacia probatoria di cui all'art. 2712 c.c., mentre altri, ai sensi dell'art. 20, comma 1-*bis*, secondo periodo, CAD, reputano il messaggio di posta elettronica privo di firma e, quindi, liberamente valutabile in sede giudiziale in ordine al suo valore probatorio e all'idoneità a soddisfare il requisito della forma scritta, in relazione alle sue caratteristiche oggettive di sicurezza, integrità e immodificabilità[47].

In considerazione di ciò, parte della dottrina[48] ha sostenuto che l'art. 20, comma 1-*bis*, secondo periodo, CAD si riferirebbe solo a quelle scritture c.d. informatiche dichiarative che «costituiscono per definizione lo strumento per compiere manifestazioni di volontà o di scienza, e cioè sono strumenti per comunicare a taluno la volontà del dichiarante oppure un dato o un fatto conosciuto da quest'ultimo». Esse si differenziano però dalle riproduzioni meccaniche, in quanto «non servono a dare forma a stati mentali altrimenti regolati nel foro interno del soggetto, quali la sussistenza di una volontà impegnativa o dello stato di conoscenza di taluni fatti». In dottrina è preponderante la tesi secondo cui alle e-*mail* espressioni di manifestazioni di volontà o di scienza, annoverabili come tali fra le scritture informatiche dichiarative, non può essere applicato il dispositivo inerente alle riproduzioni meccaniche, bensì l'art. 20, comma 1-*bis*, CAD[49]. Pertanto, alle *e-mail* c.d. ordinarie, dove non è stata apposto alcun tipo di firma (compresa quella semplice), non è applicabile la norma in tema di riproduzioni meccaniche; viceversa, a quelle munite di firma digitale, qualificata o avanzata, soddisfacendo il requisito della forma scritta[50], può essere riferita la disciplina di cui all'art. 2712 c.c. Infine, secondo le indicazioni del CAD, la *e-mail* non sottoscritta da firma digitale, qualificata o avanzata, e quindi non sottoscritta o sottoscritta tramite firma elettronica semplice, è liberamente valutabile in sede giudiziale rispetto alle caratteristiche oggettive precedentemente richiamate[51]. In altri termini, riguardo all'ambito applicativo, si può affermare che sono riconducibili all'art. 2712 c.c. tutti quei documenti informatici consistenti in registrazioni sonore, visive o audiovisive, mentre all'art. 20 CAD sono ascrivibili

[44] Art. 6, comma 5, d.P.R. n. 68/2015.
[45] GARGANO - SILENI, *Il codice del PCT commentato*, Milano 2020, 162. Nel caso di specie, la Società Citieffe S.r.l. ha prodotto in giudizio la documentazione attestante un disservizio creato dal proprio gestore PEC. Questo non è stata considerata valida giustificazione dal Giudice napoletano in quanto il disservizio non è stato costante per l'intero periodo in cui era possibile proporre opposizione, ma riferito solo a tre diversi momenti (n. 3 giorni).
[46] Cfr. COMETTO, *La valenza probatoria degli SMS*, in *Giur. it.*, 2020, 91, ove si legge: «tanto l'indirizzo di posta elettronica, quanto il numero telefonico, non sono idonei ad integrare una firma elettronica semplice».
[47] Cfr., sul punto, RICCI, *L'efficacia probatoria dell'e-mail non sottoscritta*, cit., 630-631: infatti, «anche nelle decisioni che qualificano i messaggi di posta elettronica come scritture prive di sottoscrizione: a) solo una parte della giurisprudenza ritiene che alle stesse dovrebbe attribuirsi l'efficacia probatoria delle riproduzioni meccaniche di cui all'art. 2712 c.c. (e altrettanto dovrebbe dirsi anche per gli sms, cioè per i messaggi telefonici generati tramite il c.d. *short message service*); b) secondo un altro orientamento, infatti, in applicazione dell'art. 20 d.lgs. 7 marzo 2005, n. 82, recante il «codice dell'amministrazione digitale» [...], il messaggio di posta elettronica privo di firma elettronica è liberamente valutabile dal Giudice in ordine all'idoneità a soddisfare il requisito della forma scritta, in relazione alle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità».
[48] Cfr., sul punto, CARNELUTTI, *La prova civile. Parte generale. Il concetto giuridico di prova*, Milano, 1992, 158 ss.; DE SANTIS, *Il documento non scritto come prova civile*, Napoli 1988, 23 ss.
[49] RICCI, *L'efficacia probatoria dell'e-mail non sottoscritta*, cit., 633.
[50] Art. 20, comma 1-*bis*, primo periodo, CAD.
[51] Art. 20, comma 1-*bis*, secondo periodo, CAD.

i documenti informatici «che derivano dal fatto di aver tracciato simboli grafici appartenenti ad un linguaggio su di un supporto informatico»[52].

Inoltre, sempre in tema di efficacia probatoria dei documenti informatici privi di sottoscrizione elettronica, è da sottolineare come inizialmente l'opinione dominante ritenesse di ricondurre siffatto documento non sottoscritto alla più ampia *species* delle riproduzioni meccaniche disciplinate dall'art. 2712 c.c., considerandolo quale «norma di chiusura». Questo orientamento è stato superato a seguito dell'intervento del legislatore: si è ritenuto di non poter più invocare la norma in tema di riproduzioni meccaniche, bensì l'art. 20, comma 1-*bis*, secondo periodo, CAD, il quale presenta una vocazione residuale rispetto a tutti i casi disciplinati dal primo periodo dello stesso articolo. Esso trova applicazione ogni volta che il documento informatico sia sprovvisto di una qualsiasi firma elettronica sicura[53] e non sia stato formato, previa identificazione informatica dell'autore, con un procedimento rispettoso dei requisiti tecnici definiti dalle Linee Guida dell'AgID al fine di garantire la sicurezza, l'integrità e l'immodificabilità del documento[54].

Dunque, ai sensi dell'art. 20, comma 1-*bis*, secondo periodo, CAD, «l'idoneità del documento informatico [non sottoscritto] a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle sue caratteristiche oggettive di sicurezza, integrità e immodificabilità». Trattandosi di un documento munito di firma elettronica, seppur semplice, è innegabile la differenza con un qualunque documento informatico non sottoscritto, per il quale è necessario, in sede giudiziale, indagare sulla paternità del documento. L'esistenza di una correlazione tra quest'ultimo e il suo autore è attestata dall'insieme di «dati acclusi oppure connessi tramite associazione logica al documento informatico», come descritto dall'art. 3, comma 1, n. 10 del Regolamento eIDAS. Tuttavia, vi sono casi in cui potrebbero intervenire fatti che escludono qualsiasi correlazione logica tra il documento informatico e l'apparente sottoscrittore.

Una volta accertata la provenienza del documento informatico sottoscritto, occorre valutarne il valore probatorio, secondo il principio del libero convincimento del giudice *ex* art. 20, comma 1-*bis*, secondo periodo, CAD, e tenendo in considerazione anche l'art. 21, comma 2-*bis*, CAD. Di conseguenza, il documento informatico munito di sottoscrizione elettronica semplice non può mai integrare gli estremi della forma scritta richiesti dall'art. 20, comma 1-*bis*, secondo periodo, CAD ogni volta che questa sia condizione di validità di un atto. Ad ogni modo, tale documento informatico può integrare il requisito mancante qualora la firma elettronica semplice sia imposta dalla legge *ad probationem tantum* o a qualsiasi altro fine. Difatti, «superato il preliminare vaglio giudiziale della sicurezza e sull'affidabilità del documento, non sembra esservi alcuna ragione per negare l'esistenza di una piena omogeneità tra il documento informatico munito di firma elettronica semplice e un documento cartaceo e sottoscritto»[55]. In definitiva, è possibile affermare che, a condizione che il Giudice abbia verificato la provenienza del documento informatico e lo ritenga sufficientemente affidabile in relazione alle sue caratteristiche oggettive di sicurezza, integrità e immodificabilità, lo stesso munito di sottoscrizione elettronica semplice può essere prodotto in giudizio.

Invece, per i documenti informatici muniti di sottoscrizione elettronica avanzata, qualificata e digitale, si rinvia agli artt. 20 e 21 CAD, rispettivamente riguardanti la loro efficacia probatoria e sostanziale. In particolare, l'art. 20, comma 1-*bis*, primo periodo, CAD attribuisce al documento informatico sottoscritto con una delle

[52] CERDONIO CHIAROMONTE, *Il valore dell'email*, cit., 449.
[53] Secondo il CAD, le firme considerate sicure sono quella elettronica avanzata, la qualificata e la digitale.
[54] BERTOLLINI, *Il documento informatico e il documento analogico*, in *Il processo telematico nel sistema del diritto processuale civile*, a cura di *Ruffini*, Milano 2019, 64 ss.
[55] BERTOLLINI, *Il documento informatico e il documento analogico*, cit., 69. L'art. 21, comma 2-*bis*, CAD subordina alla presenza della firma digitale o di altro tipo di firma elettronica qualificata la validità dei principali contratti (*ex* art. 1350, comma 1, n. 1-12, c.c.) conclusi in formato elettronico. Diversamente, gli altri atti previsti dall'art. 1350, comma 1, n. 13, c.c. «necessitano di una firma elettronica avanzata, oppure devono essere stipulati con un documento informatico privo di firma elettronica, ma che sia stato generato nel rispetto delle procedure tecniche stabilite dall'AgID, ai sensi dell'art. 20, comma 1-*bis*, primo periodo, CAD».

c.d. firme elettroniche sicure l'efficacia probatoria della scrittura privata, *ex* art. 2702 c.c., dove il comma 1-*ter* aggiunge che «l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare di firma elettronica, salvo che questi dia prova contraria»[56]. Sul punto, un primo orientamento[57] equipara l'efficacia probatoria del documento munito di una delle firme elettroniche sicure a quella delle scritture private cartacee. Sembrerebbe, infatti, che l'art. 20, comma 1-*bis*, primo periodo, CAD richiami l'intera disciplina in materia di scritture private, includendo le disposizioni che regolano l'onere di disconoscimento e la successiva procedura di verifica. Di conseguenza, un documento informatico siffatto farebbe piena prova «fino a querela di falso, della provenienza delle dichiarazioni in esso contenute da parte di colui che l'ha sottoscritto, a condizione che la firma sia stata riconosciuta o debba essere legalmente considerata tale»[58]. Infatti, ai sensi dell'art. 214 c.p.c., la parte contro la quale è prodotto il documento informatico ha l'onere di disconoscerne la sottoscrizione nella prima udienza o nella risposta successiva alla produzione; successivamente, la controparte ha l'onere di chiedere la verifica e di dimostrare l'autenticità della firma (art. 216 c.p.c.).

Il secondo orientamento[59], invece, attribuisce al documento munito di firma elettronica avanzata, qualificata o digitale un'efficacia probatoria «assimilabile a quella delle scritture private riconosciute o legalmente considerate tali»[60]. Il richiamo al disposto del codice civile avrebbe la mera funzione di evocare l'efficacia di prova legale e non anche tutte le norme che regolano il disconoscimento e la verifica delle scritture; ne segue che il documento informatico sottoscritto mediante le c.d. firme elettroniche sicure farebbe piena prova, fino a querela di falso, della provenienza delle dichiarazioni da parte di colui che l'ha sottoscritto, indipendentemente dal riconoscimento (espresso o tacito) di quest'ultimo. Sotto il profilo procedurale, è onere della controparte proporre querela di falso contro l'efficacia probatoria del documento informatico e dimostrare la falsità dello stesso e/o della sottoscrizione elettronica.

In sostanza, la prima interpretazione dell'art. 20, comma 1-*bis*, primo periodo, CAD ritiene che l'efficacia probatoria del documento informatico possa essere rimossa attraverso il disconoscimento della scrittura digitale; viceversa, la seconda pone in capo alla controparte l'onere di proporre querela di falso. Entrambi gli orientamenti sono rispettosi del dettato normativo e, quindi, trattandosi di discrezionalità principalmente interpretativa, si può concludere che la contrapposizione sia da considerare più apparente che concreta.

In riferimento all'efficacia sostanziale del documento informatico sottoscritto dalle c.d. firme sicure, l'art. 21, comma 2-*bis*, CAD stabilisce che i contratti di cui all'art. 1350, comma 1, n. 1-12, c.c. possono essere stipulati in via telematica solo se vi è apposta una firma elettronica qualificata o digitale. Di conseguenza, si ritiene nullo il contratto solenne privo di una di queste due firme elettroniche. Al

[56] Cfr. ORLANDI, *Il falso digitale*, cit., 130.

[57] Cfr. BUONOMO - MERONE, *La scrittura privata informatica: firme elettroniche, valore probatorio e disconoscimento in giudizio [alla luce delle modifiche introdotte dalla 1. 221/2012]*, in *Judicium, Il processo civile in Italia e in Europa*, 2013; LISI - SCIALDONE, Il d*ocumento informatico e le firme elettroniche*, in *Diritto dell'internet e delle nuove tecnologie telematiche*, a cura di Cassano e Cimino, Padova 2002, 449 ss.; MERONE, *Il disconoscimento delle prove documentali*, Torino 2018, 217 ss.; PATTI, *L'efficacia probatoria del documento informatico*, in *Riv. dir. proc.*, 2020, 68 ss.; RICCI, *Scritture private e firme elettroniche*, Milano 2003, 238-239; VERDE, *Per la chiarezza di idee in tema di documentazione informatica*, in *Riv. dir. proc.*, 1990, 715 ss.

[58] BERTOLLINI, *Il documento informatico e il documento analogico*, cit., 70.

[59] Cfr. BIANCA, *Diritto civile. Il contratto*, III, Milano 2019, 305 ss.; COMOGLIO, *Le prove civili*, Torino 2010, 553-554; FERRARI, *I codice dell'amministrazione digitale e le norme dedicate al documento informatico*, in *Riv. dir. proc.*, 2007, 425-426; FINOCCHIARO, *Alcune riflessioni sull'uso abusivo della chiave privata nell'apposizione della firma digitale*, in *Scrittura e diritto. Quaderni della Rivista trimestrale di diritto e procedura civile*, 2000, 211 ss.; GENTILI, *Documento informatico e tutela dell'affidamento*, in *Riv. dir.civ.*, 1998, II, 163 ss., spec. 171 ss.; ID., *Negoziare* on line *dopo la riforma del codice dell'amministrazione digitale*, in *Corriere mer.*, 2011, IV, 354; ID., voce *Documento informatico (dir. civ.)*, in *Enc. dir. Annali*, V, Milano, 2012, 629 ss., spec. 653 ss.; GRAZIOSI, *Premesse ad una teoria probatoria del documento informatico*, in *Riv. trim. dir. proc. civ.*, 1998, 514 ss.; ID., voce *Documento informatico (dir. proc. civ.)*, in *Enc. dir. Annali*, II, Milano, 2008, 491 ss.; MANDRIOLI - CARRATTA, *Diritto processuale civile*, II, Torino, 2017, 238; TARUFFO, *Parola scritta e parola informatica nel processo civile*, in AA. VV., *Scrittura e diritto*, Milano, 2000, 91 ss.

[60] BERTOLLINI, *Il documento informatico e il documento analogico*, cit., 70.

contrario, gli altri atti a forma vincolata *ex* art. 1350, comma 1, n. 13, c.c. «possono essere conclusi in formato informatico solo se il documento, che li contiene, è munito di firma elettronica avanzata oppure se, pur non essendo sottoscritto, esso è stato generato nel rispetto delle procedure tecniche stabilite dall'AgID ai sensi e per gli effetti dell'art. 20, comma 1-*bis*, primo periodo, c.a.d.»: in mancanza anche solo di uno di questi requisiti, il negozio giuridico è da dichiararsi nullo[61].

In definitiva, si può affermare che qualsiasi contratto sia suscettibile di essere stipulato attraverso un documento informatico munito di firma elettronica digitale o qualificata, ad eccezione di quelli che richiedono l'atto pubblico o la scrittura privata autenticata. Invece, la firma elettronica avanzata apposta su un documento può essere utilizzata per concludere atti che non richiedano particolari requisiti e negozi giuridici a forma vincolata di cui all'art. 1350, comma 1, n. 13, c.c. In altri termini, «non tutte le sottoscrizioni elettroniche sono idonee a soddisfare il requisito della forma scritta *ad substantiam*, dando luogo nel nostro ordinamento ad un fenomeno di "gradazione" della validità della scrittura privata elettronica». In particolare, i documenti informatici muniti di sottoscrizione semplice non possono essere in alcun modo considerati capaci di soddisfare il requisito della forma scritta a pena di nullità[62].

In conclusione, ai sensi dell'art. 20, comma 1-*bis*, primo periodo, CAD, è possibile affermare che i documenti informatici muniti di sottoscrizione sicura sono da considerarsi pienamente idonei a soddisfare il requisito della forma scritta al punto che possono essere utilizzati in giudizio per dimostrare l'esistenza dei negozi giuridici per i quali sia richiesta la forma scritta *ad probationem tantum*[63].

5. (SEGUE): LA PEC

L'art. 48, comma 2 e 3[64] e l'art. 6 comma 1 del d.lgs. n. 82/2005 equiparano la trasmissione di un documento informatico tramite PEC alla notificazione a mezzo posta, precisando che la data e l'ora di trasmissione e di ricezione di un messaggio di posta elettronica certificata è opponibile a terzi, con il solo limite della non conformità di tale marcatura temporale alle disposizioni previste dalle Linee guida AgID.

In base a tale parificazione, ci si domanda se sia necessario stabilire se l'efficacia probatoria della ricevuta di accettazione e della ricevuta di avvenuta consegna corrisponda all'efficacia probatoria della relata di notifica e dell'avviso di ricevimento e sia, quindi, riconducibile all'efficacia di piena prova fino a querela di falso[65]. Siffatta ipotesi sembra doversi escludere perché elemento distintivo dell'atto pubblico è la materiale sottoscrizione di un ufficiale pubblico che attesti le operazioni compiute in sua presenza, elemento che non è, invece, riscontrabile in messaggi generati automaticamente da un sistema informatico, benché sottoscritti con firma elettronica avanzata. Poiché il gestore di posta elettronica certificata, che sottoscrive la ricevuta di avvenuta accettazione e di avvenuta consegna, è una persona giuridica, la sua attività non sembra equiparabile a quella di un pubblico ufficiale che - per sua natura - è soltanto una persona fisica. Per di più, tali ricevute sono generate in maniera automatica da un sistema informatico e, quindi, non necessitano dell'attività dichiarativa o certificativa di un pubblico ufficiale[66].

[61] BERTOLLINI, *Il documento informatico e il documento analogico*, cit., 72.
[62] BRAVO, *Sull'obbligo di copertura assicurativa a carico dei soggetti che "erogano" soluzioni di firma elettronica avanzata*, in *Dir. Informatica*, 2017, 677-678.
[63] Cfr., sul punto, BERTOLLINI, *Il documento informatico e il documento analogico*, cit., 73; LISI - SCIALDONE, Il d*ocumento informatico e le firme elettroniche*, cit., 461 ss.; SCARPA, *Riflessioni sull'e-mail come possibile prova scritta cit.,* 7 ss.
[64] L'art. 48, d.lgs. n. 82/2005 è stato abrogato per effetto della previsione contenuta nell'art. 8, comma 5, d.l. n. 135/2018.
[65] PORCELLI, *La posta elettronica certificata*, cit., 124 s., in part. nota 98. «La giurisprudenza attribuisce alla relata di notifica apposta sulla copia e sull'originale dell'atto notificato e all'avviso di ricevimento valore di atto pubblico per la qualità degli autori [...] e per la funzione pubblica di certificazione degli stessi esplicata».
[66] PORCELLI, *La posta elettronica certificata*, cit., 125 ss. «In radice, infatti, occorre osservare che tanto la ricevuta di accettazione, quanto la ricevuta di avvenuta consegna recano la firma elettronica avanzata del gestore di PEC (e quindi di una persona giuridica), automaticamente apposta da un sistema informatico. Al riguardo non sembra davvero possibile ritenere, anche nell'era dell'innovazione tecnologica, che un sistema informatico possa rivestire la qualità di pubblico ufficiale».

A tal proposito, la Corte di Cassazione[67] ha dichiarato che l'art. 48, comma 2, d.lgs. n. 82/2005 assimila la PEC alla notifica a mezzo posta esclusivamente con riguardo «all'efficacia giuridica di questa forma di trasmissione dei documenti elettronici», ma ciò non varrebbe «a rendere applicabile l'intera disciplina prevista dalla l. 20 novembre 1982, n. 890 [...], dovendosi sul punto sottolineare che il gestore di posta elettronica certificata [...] rimane comunque un soggetto privato [...], quindi, naturalmente privo del potere di attribuire pubblica fede, ai sensi dell'art. 2699 c.c., ai propri atti».

Alla luce di tali osservazioni, pare opportuno ritenere che la documentazione dei messaggi di PEC non abbia efficacia probatoria privilegiata e che, pertanto, non sia necessaria la proposizione della querela di falso. Perciò, occorre individuare una modalità per contestare l'efficacia probatoria delle ricevute generate automaticamente dal gestore di posta elettronica certificata.

In via preliminare, è necessario precisare che la tempestività della spedizione e/o il perfezionamento della trasmissione di un messaggio a mezzo PEC devono essere dimostrati depositando telematicamente il duplicato analogico o la copia informatica di tale documentazione[68]. Ciò premesso, è opportuno distinguere tra contestazioni relative al difetto di conformità all'originale della documentazione prodotta in giudizio - in formato cartaceo o elettronico - e contestazioni relative all'efficacia probatoria di tale documentazione.

Per quanto riguarda l'ipotesi in cui sia prodotta in giudizio la stampa cartacea delle ricevute dei messaggi di PEC, tale documento costituisce copia analogica di un documento informatico, tenendo conto che sia le ricevute menzionate sia il messaggio di PEC originario sono documenti informatici. Ai sensi dell'art. 23 d.lgs. n. 82/2005, le copie su supporto analogico di un documento informatico hanno la stessa efficacia probatoria dell'originale da cui sono tratte «se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato», ma, in ogni caso, «l'efficacia certificativa della PEC non si estende[rà] al profilo della conformità all'originale delle copie analogiche delle ricevute di avvenuta consegna o accettazione»[69]. Di conseguenza, al fine di individuare le modalità per contestare la conformità delle citate copie analogiche all'originale, occorre far riferimento alla disciplina concernente l'efficacia probatoria delle copie analogiche dei documenti informatici[70]. Laddove, invece, si tratti di un messaggio PEC attestante una notificazione, come nel caso di specie, l'attestazione dell'avvocato incaricato è sufficiente ad attribuire pubblica fede alla conformità della copia all'originale prodotto telematicamente e, nel caso in cui si voglia contestare tale conformità, sarà necessaria la querela di falso.

Diversamente, nell'ipotesi in cui venga provata tramite modalità telematiche l'avvenuta spedizione e ricezione di un messaggio di posta elettronica certificata, il mittente potrà depositare il duplicato dei documenti informatici attestanti l'avvenuta accettazione e l'avvenuta consegna[71].

Al di fuori delle ipotesi appena menzionate di contestazioni della conformità all'originale (riferite alla copia su supporto analogico o informatico oppure del duplicato della ricevuta di accettazione e della ricevuta di avvenuta consegna), si devono individuare ipotesi di contestazione relative all'efficacia probatoria delle ricevute dei messaggi trasmessi a mezzo PEC.

[67] Cass. 21 luglio 2016, n. 15035, in *Fall.*, 2017, 184 ss.

[68] PORCELLI, *La posta elettronica certificata*, cit., 126 s. «Detta soluzione è legislativamente obbligata per le ricevute di messaggi PEC relativi a notificazioni, ma deve essere estesa ad ogni messaggio di posta elettronica certificata. Solo laddove il deposito telematico dei *file* non sia possibile, il difensore provvederà a stampare il contenuto del messaggio e delle ricevute e ad attestare la conformità all'originale telematico».

[69] PORCELLI, *La posta elettronica certificata*, cit., 127 s. Sul punto, cfr. anche BONAFINE, *L'atto processuale telematico. Forma, tipologie, sanatorie*, Napoli 2017 e ROSSETTI, MURATORE, SANTOPIETRO, *Il processo esecutivo telematico*, Milano 2016, 10 ss.

[70] Infatti, l'art. 23 CAD, comma 2 stabilisce che «le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico».

[71] Il duplicato di documenti informatici ha lo stesso valore giuridico del documento informatico da cui è tratto, se prodotto in conformità alle Linee Guida AgID (art. 23 CAD). Di conseguenza, qualora si contesti che il duplicato informatico non sia stato generato secondo le conformità richieste di cui all'art. 71 d.lgs. n. 82/2005, occorre fa riferimento alla disciplina in ordine all'efficacia probatoria del duplicato informatico.

Avendo stabilito che detti documenti non presentano efficacia probatoria privilegiata, si deve escludere la possibilità di proporre querela di falso per avanzare contestazioni aventi ad oggetto la data, l'orario e l'oggetto del messaggio spedito dal mittente. Tuttavia, potranno essere provate liberamente la mancata ricezione del messaggio PEC o la ricezione a una data o a un'ora diverse da quelle certificata dalla marcatura temporale generata automaticamente dal gestore. In altre parole, nel caso in cui si contesti la data o l'ora, potrà essere prodotta in giudizio dalla parte, o richiesta direttamente dal Giudice, la documentazione attestante la non conformità.

Nel caso in cui, invece, la contestazione sia relativa al contenuto della PEC o alla mancata ricezione è necessario tener presente che esistono tre tipologie di ricevuta di avvenuta consegna: completa[72], breve[73] e sintetica[74]. Con riferimento alle prime due tipologie di ricevuta di consegna, è onere del destinatario provare la difformità tra il contenuto della ricevuta e quella prodotta in giudizio dal mittente. Al contrario, nel caso di ricevuta di consegna sintetica, il destinatario può limitarsi a negare di aver ricevuto un *file* in allegato al messaggio trasmesso a mezzo PEC, gravando così sul mittente l'onere di dimostrare l'avvenuta spedizione e l'avvenuta consegna degli allegati[75].

6. *SPUNTI FINALI DI COMPARAZIONE*

Dopo aver analizzato alcuni aspetti che differenziano da un punto di vista sostanziale e procedurale la posta elettronica ordinaria da quella certificata, è opportuno operare un confronto diretto e trarre qualche conclusione.

Risulta chiaro, a partire dal nome, che la PEC è un sistema di trasmissione elettronica più sicuro rispetto alla *e-mail* e per questo motivo è stato elevato a metodo di notifica degli atti giudiziari, perché in grado di garantire l'avvenuta ricezione grazie alla ricevuta di accettazione e a quella di avvenuta consegna. Infatti, il valore giuridico della *e-mail* priva di sottoscrizione elettronica è liberamente valutabile in sede giudiziale dal Giudice in ordine all'idoneità a soddisfare il requisito della forma scritta, in relazione alle sue caratteristiche oggettive di sicurezza, integrità e immodificabilità[76], mentre la PEC - essendo contraddistinta da un sistema che assicura la ricezione del messaggio - ha piena efficacia probatoria salvo che la parte dimostri che la mancata ricezione non sia dipesa da fatto proprio, bensì da caso fortuito o forza maggiore.

Una seconda peculiarità che rende la posta elettronica certificata più sicura rispetto alla *e-mail* ordinaria è l'identificazione del soggetto (sia esso il mittente o il destinatario). In particolare, come si è già visto, la PEC può essere facilmente riconducibile a uno degli elenchi pubblici, mentre non esiste alcun sistema in grado di identificare l'utente sottoscrittore dell'*e-mail* ordinaria.

[72] Ai sensi degli artt. 6, comma 4, d.P.R. n. 68/2005 e 1, comma 1, lett. *i*), d.m. n. 19818/2005, la ricevuta di avvenuta consegna *completa* contiene sia il messaggio originale per intero che gli allegati.

[73] La ricevuta di avvenuta consegna *breve* contiene un *hash* (ossia, ai sensi dell'art. 1, lett. *g*) d.P.C.M. 30 marzo 2009, «una funzione matematica che genera, a partire da una evidenza informatica, un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti») sia per l'estratto del messaggio originale sia per gli eventuali allegati.

[74] La ricevuta di avvenuta consegna sintetica non contiene né il messaggio originale (per esteso o per estratto) né tantomeno gli allegati relativi.

[75] Cfr. DI GIACOMO, *Il nuovo processo civile telematico*, Milano 2015, 170 ss.; TAFFARI, Il *processo civile telematico*, cit., 70 ss. In particolare, PORCELLI, *La posta elettronica certificata*, cit., 130. La soluzione che prevede l'onere della prova in capo al mittente, rende «in concreto più difficile l'esercizio del diritto di difesa [...], ma la stessa non lede tale diritto, atteso che il mittene stesso ben potrebbe [...] precostituirsi la prova del contenuto del messaggio di PEC e dell'eventuale esistenza di documenti informatici allegati, optando per la ricevuta di avvenuta consegna completa e breve; con un risultato analogo a quello raggiungibile dal mittente che, per evitare le conseguenze derivanti dalle eventuali contestazioni del destinatario, sceglie di spedire una lettera raccomandata con avviso di ricevimento in piego raccomandato senza busta». Inoltre, viene rilevato che il fatto oggetto della prova si è in realtà prodotto nella sfera giuridica del mittente, così da averne non solo diretta conoscenza, ma anche disponibilità degli elementi per dimostrare l'esistenza o meno del fatto controverso. Tale riconducibilità al mittente, potrà essere elevata da parte del Giudice a criterio di ripartizione dell'onere della prova, qualora tale fatto sia rimasto sprovvisto di prova ossia quando il destinatario non sia riuscito a fornire la prova delle diversità del messaggio trasmesso a mezzo PEC originario da quello prodotto in giudizio dal mittente, oppure quando non sia riuscito a dimostrare di aver ricevuto un messaggio di PEC privo di contenuto e di non aver ricevuto alcun documento. In ogni caso, tali ipotesi svaniscono qualora il destinatario riconosca espressamente di aver ricevuto il messaggio di PEC e il documento informatico allegato al citato messaggio, che il mittente ha prodotto in giudizio.

[76] Art. 20, comma 1-*bis*, secondo periodo, CAD.

Infine, ultima caratteristica che contraddistingue i due sistemi di posta elettronica è la certezza in merito al contenuto del messaggio. Come evidenziato nella decisione del Tribunale di Milano, può risultare relativamente semplice cambiare il testo di un messaggio una volta spedito, dal momento che, quando si 'risponde' a una *e-mail* o la si 'inoltra', quest'ultima può essere modificata in calce alla *e-mail* che si intende scrivere. Ciò non può avvenire, invece, con l'invio di messaggi di posta elettronica certificata, i quali non possono essere modificati, neanche in sede di risposta o di inoltro.

In conclusione, il sistema di posta elettronica certificata non soltanto deve essere utilizzato nei casi in cui la legge lo prevede, ma il suo impiego è altresì preferibile allorché si vogliano trasmettere comunicazioni di una certa rilevanza.