

**Analisi degli strumenti informatici per la  
digitalizzazione e informatizzazione della  
Pubblica Amministrazione e dei suoi rapporti  
con i cittadini e le imprese: lo stato dell'arte**

## Sommario

INTRODUZIONE.....	1
PEC FIRMA ELETTRONICA MARCA TEMPORALE .....	3
Una questione terminologica.....	3
Cosa sono PEC, Firma Elettronica e Marca Temporale .....	3
PEC e firma digitale non sono la stessa cosa!.....	6
Identificazione e sottoscrizione.....	7
NORMATIVA DI RIFERIMENTO .....	9
Considerazioni in merito al modo di normare.....	16
Il caso particolare dei documenti classificati .....	16
Legislazione delegata: pregi e limiti .....	18
Le Regole tecniche: pro e contro .....	19
Le Circolari: uso e abuso .....	23
LA PEC .....	25
<b>Brevissima storia .....</b>	25
<b>Caratteristiche salienti e giuridicamente rilevanti.....</b>	25
<b>Cosa è una PEC? Una busta!</b> .....	25
<b>Avvisi delle PEC, Ricevute, Buste.....</b>	27
<b>Gli allegati della PEC .....</b>	28
<b>Obbligo della PEC .....</b>	29
<b>Obbligo per i cittadini.....</b>	29
<b>Obbligo per professionisti e imprese .....</b>	30
<b>Obbligo per la PA .....</b>	30
La conservazione dei messaggi e delle ricevute di PEC .....	31

<b>La conservazione dei dati “a norma di legge” .....</b>	32
<b>Vari tipi di PEC .....</b>	34
<b>Elenchi PEC .....</b>	37
<b>PUNTI CRITICI della PEC .....</b>	40
LA FIRMA ELETTRONICA .....	43
Il documento informatico ed il documento amministrativo .....	46
Le definizioni di “firma”:.....	49
La firma digitale ed il suo funzionamento tecnico.....	53
Il caso della firma automatica .....	54
Il caso della firma da remoto.....	55
La firma autografa elettronica: un caso speciale.....	55
Casi in cui la firma elettronica può essere sostituita da altri strumenti (CIE, TS, CNS, SPID) .....	58
PEC e FIRMA ELETTRONICA nel processo telematico .....	61
LA MARCA TEMPORALE .....	66
Come eIDAS modifica PEC, firma elettronica e marca temporale .....	69
Cosa è eIDAS .....	69
Limiti nell’applicabilità di eIDAS e suo valore giuridico.....	72
Modifiche riguardo alla PEC .....	76
Modifiche riguardo alla Firma Elettronica.....	78
Modifiche riguardo alla Marca Temporale .....	81
eIDAS e il sigillo elettronico.....	82
Come il nuovo CAD modifica PEC, firma elettronica e marca temporale .....	85
Cosa intendiamo per nuovo CAD .....	85
Modifiche riguardo alla PEC .....	88
Modifiche riguardo alla Firma elettronica .....	92
Modifiche riguardo alla Marca temporale.....	93
SENTENZE ESEMPLARI .....	94

Introduzione .....	94
Caso 1 Il Consiglio di Stato .....	95
Caso 2 La firma digitale nel giudizio della Cassazione .....	97
Caso 3 Inesistente la notifica tramite pec senza la ricevuta di avvenuta consegna.....	99
Caso 4 Il destinatario dell'atto non può eccepire di non aver letto il messaggio.....	100
Caso 5 PEC valida anche senza firma elettronica.....	101
Caso 6 Notifica con PEC inutile se l'azienda non ha la firma digitale .....	104
Considerazioni sulle sentenze analizzate .....	105
CONCLUSIONI.....	106
ABBREVIAZIONI .....	108
BIBLIOGRAFIA .....	109

## INTRODUZIONE

In questo lavoro ci proponiamo di analizzare cosa sono e come funzionano alcuni degli strumenti informatici che permettono di sostituire in *toto* o in parte la corrispondenza cartacea "qualificata" ovvero quella avente valore legale e probatorio e che quindi risultano indispensabili nell'opera di smaterializzazione e digitalizzazione che ormai pare inevitabile e necessaria in tutti i campi e in particolare nella Pubblica Amministrazione (PA).

Si tratta in della PEC (posta elettronica certificata), della firma elettronica (FE) e della marca temporale (MT).

Di questi strumenti elettronici verrà brevemente illustrato il funzionamento e gli aspetti tecnici (limitatamente a quanto necessario per comprenderne le implicazioni giuridico-legali, anche in considerazione del fatto che come per tutti i campi ormai *la Rete* permette di trovare con facilità i dettagli più strettamente tecnici ) e verranno illustrati i presupposti giuridico normativi che ne permettono e disciplinano l'uso, con un cenno al modo di legiferare in questa materia che presenta diversi aspetti interessanti, sia riguardo all'uso massiccio in questo campo della legislazione delegata, sia riguardo alla necessità di emanazione di "Norme tecniche" senza le quali sembra impossibile applicare comiutamente la normativa, sia infine riguardo alla importanza che spesso assumono le Circolari.

Saranno poi analizzati i rapporti tra PEC FE MT e le recenti disposizioni in materia di privacy e riconoscimento biometrico, le connessioni con il più generale concetto di documento digitale, con l'introduzione della Anagrafe Nazionale della Popolazione Residenti (ANPR) e del Sistema Pubblico per la gestione dell'Identità Digitale (SPID).

Saranno analizzati i cambiamenti che comporta l'entrata in vigore del regolamento europeo eIDAS (electronic IDentification Authentication and Signature) e le ricadute dei recentissimi provvedimenti adottati dal Governo nell'ambito della Legislazione Delegata riguardante la PA e che promettono di modificare in modo radicale la normativa in questo campo, in particolare lo SCHEMA DI DECRETO LEGISLATIVO RECANTE MODIFICHE E INTEGRAZIONI AL CODICE

DELL'AMMINISTRAZIONE DIGITALE DI CUI AL DL 7 MARZO 2005, N. 82, AI SENSI DELL'ART. 1 DELLA LEGGE 7 AGOSTO 2015, N. 124, (da qui in avanti SCHEMA DL 20/01/2016) approvato in via preliminare dal Consiglio dei Ministri in data 20 gennaio 2016, che sta seguendo il suo iter verso la definitiva emanazione e che comunque entrerà in vigore, così come il Regolamento eIDAS, il 1° luglio 2016. Infatti, anche se si tratta di un provvedimento ancora oggetto di diverse critiche anche da parte delle istanze che sono tenute a dare un parere, peraltro non vincolante, i cambiamenti da esso apportati, soprattutto nel tentativo di adeguare il CAD (Codice dell'Amministrazione Digitale) al citato Regolamento europeo, sono così rilevanti che non è possibile non tenerne conto in questa trattazione.

Verranno infine analizzate alcune recenti sentenze, allo scopo di illustrare la giurisprudenza in materia ed introdurre elementi di riflessione sulla applicazione e sulla applicabilità della normativa.

In tutta la trattazione, data la natura della normativa, oggetto di continui aggiornamenti e modifiche, si è fatto riferimento ai diversi siti (governo<sup>1</sup>, agenzia digitale<sup>2</sup>, etc.) dove sono riportate le norme e alcuni commenti o precisazioni. Per la parte tecnica si fa riferimento soprattutto al citato sito della Agenzia per l'Italia Digitale (AgID). Per la parte più strettamente giuridica (testo delle norme, testo in vigore, modifiche, circolari etc.) si fa riferimento soprattutto al sito [www.normattiva.it](http://www.normattiva.it) che, realizzato e gestito dall'Istituto Poligrafico dello Stato, riporta il "testo vigente" delle normative con l'ovvia avvertenza che solo la Gazzetta Ufficiale, i testi ivi riportati e il relativo sito<sup>3</sup> di cui pure si è fatto uso, sono le fonti uniche con valore legale.

---

<sup>1</sup> <http://www.governo.it/>

<sup>2</sup> [www.agid.gov.it/](http://www.agid.gov.it/)

<sup>3</sup> [www.gazzettaufficiale.it/](http://www.gazzettaufficiale.it/)

## PEC FIRMA ELETTRONICA MARCA TEMPORALE

### Una questione terminologica

La dicitura *firma digitale* può ingenerare più di un equivoco. Infatti l'attributo digitale ha una connotazione, in italiano, come in quasi tutte le lingue, molto generale (si pensi a locuzioni come “*mondo digitale*”, “*digital divide*”, “*digital first*” etc). Tuttavia nella normativa italiana la dicitura *firma digitale* non indica genericamente una firma di tipo elettronico, contrapposta alla classica firma analogica, ma si riferisce ad uno specifico tipo di firma elettronica definita nel CAD in modo molto analitico<sup>4</sup> (addirittura si specifica quale deve essere l'implementazione tecnica e si indica il metodo della doppia chiave asimmetrica). Al fine di evitare fraintendimenti perciò in questo lavoro parleremo di **firma elettronica** quando si farà riferimento ad una generica forma di firma apposta usando metodi elettronici, come software dedicato o dispositivi quali chiavette, schede o tavolette grafiche o semplici coppie password/Id, mentre riserveremo il termine **firma digitale** allo specifico tipo di firma elettronica come sopra definita. Si tratta di una questione che travalica il fatto terminologico e affonda le radici in una adozione tempestiva della firma elettronica da parte del legislatore italiano che però si porta dietro l'adozione di un termine di carattere molto generale per indicare invece uno strumento particolare molto specifico. e probabilmente potrebbe risolversi usando più correttamente i termini firma elettronica avanzata e firma elettronica qualificata. Purtroppo l'attributo digitale viene praticamente sempre usato anche in riferimento alla firma elettronica in senso più generale e questo può provocare fraintendimenti anche non di poco conto.

### Cosa sono PEC, Firma Elettronica e Marca Temporale

La Posta Elettronica Certificata e la Firma Elettronica sono strumenti informatici nati per usi diversi anche se talora si tende a considerarli quasi sinonimi. In realtà si tratta di strumenti concettualmente molto diversi

---

<sup>4</sup> All'art.1 del CAD, lettera s) si definisce: *firma digitale: un particolare tipo di firma qualificata elettronica avanzata basata su un certificato qualificata e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario 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.*

Infatti la **posta elettronica certificata** è uno strumento informatico per spedire documenti da una casella di posta certificata ad un'altra casella di posta certificata. Il fatto che la spedizione avvenga tra due caselle di posta certificate garantisce la data della spedizione, l'avvenuta spedizione e l'avvenuta ricezione. Questo, unito al fatto che la certificazione delle caselle va effettuata secondo procedure stabilite dalla legge e che la trasmissione avviene con protocolli e metodi di criptaggio anch'essi stabiliti da una apposita normativa, dà alla corrispondenza spedita con la PEC valore legale e valore probatorio. (Per questo spesso si dice che la PEC è l'equivalente digitale di una raccomandata con ricevuta di ritorno). Più avanti si accennerà agli aspetti più strettamente tecnici della PEC, almeno per la parte necessaria a comprendere le implicazioni giuridico legali insite nell'uso della PEC e i contenziosi che ne possono nascere. Infatti a fronte di una apparente semplicità (e indubbiamente l'uso della PEC è molto semplice per l'utente finale, almeno in assenza di inconvenienti tecnici) la PEC nasconde particolarità tecniche molto complesse e l'invio consiste in realtà in numerosi eventi successivi ognuno dei quali deve avvenire secondo protocolli molto rigidi.

La **firma elettronica** è uno strumento elettronico che permette di attribuire "paternità certa" ad un documento digitale. In questo senso si dice che sostituisce la firma autografa più o meno autenticata. Come nel caso della PEC, l'apposizione della firma digitale, che in genere prevede apparecchiature e software particolari, è in realtà un processo tecnico piuttosto complesso. Anche per la firma digitale si darà nel seguito un breve cenno alle caratteristiche tecniche al fine di farne comprendere le implicazioni giuridiche e i vari problemi che possono nascere dal suo uso.

La **marca temporale** è uno strumento elettronico che garantisce che un particolare documento è stato compilato in una data specifica, certa e non modificabile. Anche l'apposizione della marca temporale necessita di strumenti e software studiati ad hoc, oltre a enti certificatori ufficiali, rinvenibili in appositi elenchi pubblicati ed aggiornati ufficialmente. Normalmente una marca temporale viene realizzata mediante l'apposizione della firma elettronica completa di data e ora di un ente certificatore. Poiché la Marca Temporale permette di associare una data ed un'ora certa ad un determinato documento fornisce al documento

medesimo una validazione temporale utilizzabile nei casi di controversia legale<sup>5</sup> ed assume un valore rilevante nella questione della conservazione documentale.

Che si tratti di strumenti complessi è dimostrato dal fatto che si sta generando un contenzioso ed una giurisprudenza sempre più vasta su questi argomenti, soprattutto in campo legale (la PEC può sostituire o integrare altre metodologia di notifica ed assumere un posto di rilievo nell'ambito del cosiddetto processo telematico), in campo tributario (notifica di ricorsi da parte di imprese e cittadini), nei rapporti tra cittadini, imprese e Pubblica Amministrazione, nei rapporti tra diverse istanze della PA, nei rapporti tra soggetti privati, siano essi semplici cittadini o imprese.

Già dalle sommarie definizioni riportate (le definizioni riportate nella normativa di riferimento, quelle per così dire "ufficiali" sono molto più complesse e saranno riportate più oltre) si comprende come gli strumenti informatici citati siano in qualche modo connessi tra loro e interdipendenti. E' chiaro infatti che un documento digitale inviato con la PEC può avere o meno firma digitale e marca temporale e addirittura la legge prevede casi in cui in realtà la PEC, se rispondente a certe caratteristiche può sostituire la firma digitale (ciò avviene in particolare nei casi di identificazione univoca del mittente e in questo caso si parla, nella legislazione italiana di PEC ID)<sup>6</sup>.

Appare anche ovvia la forte connessione tra gli strumenti citati e i concetti più generali di documento informatico e di identità digitale, così come è evidente il legame col più generale processo di digitalizzazione della pubblica amministrazione, dato che la PEC diventa lo strumento principale per comunicare con la Pubblica Amministrazione in tutte le sue istanze in modo sicuro, riservato e tracciabile. Non a caso la normativa prevede l'obbligo, praticamente per chiunque eserciti una attività d'impresa o una professione, di dotarsi di una PEC (lo stesso

---

<sup>5</sup> art. 20 comma 3 D.Lgs. 82/2005 , Codice dell'Amministrazione Digitale

<sup>6</sup> Tutto il DPCM del 27 settembre 2012 è dedicato a specificare le caratteristiche della PEC che integra in sé la firma digitale, ovvero la cosiddetta PEC ID

obbligo vale come è ovvio per tutte le articolazioni della PA possibili destinatarie di rapporti con soggetti esterni o interni alla PA medesima)<sup>7</sup>.

### **PEC e firma digitale non sono la stessa cosa!**

Va detto che non mettere in rilievo in modo chiaro le differenze tra PEC e firma digitale e non esplicitare tali differenze, non solo nelle normative di riferimento ma anche nelle norme tecniche, può portare a fraintendimenti e conseguenti contenziosi molto gravi. In particolare deve essere sempre chiaro che la PEC, almeno per come è definita nella normativa è il “veicolo” che trasporta un documento informatico (qui inteso nel senso più ampio) e può dare certezza sull'avvenuto invio, mentre la firma digitale attribuisce paternità certa ad un documento.

Anche se non è quasi mai corretto, anzi talvolta risulta fuorviante, fare analogie con gli strumenti “cartacei”, è un po’ come confondere la busta di una raccomandata con la firma apposta sul documento (eventualmente) contenuto nella busta. (E basta ricercare tra gli aneddoti dei vari tribunali per trovare decine di esempi di raccomandate perfettamente inviate dal punto di vista dei tempi e delle modalità di invio ma altrettanto perfettamente vuote quanto al contenuto della busta o al più contenenti un bel foglio bianco).

Questa confusione peraltro sembra sussistere anche presso alcuni tribunali come dimostra il caso della sentenza n. 1450/2015 del Tribunale Amministrativo Regionale Campano che si è pronunciato con una sentenza che riconosce validità ad alcune istanze (comunicazione e documenti allegati) inviate da un comune campano alla regione tramite PEC ma sprovviste di firma digitale (la sentenza sarà commentata in dettaglio nel capitolo “Sentenze esemplari”).

Problema analogo si pone a proposito del rapporto tra la comunicazione direttamente contenuta nel testo della PEC, gli allegati della medesima, il tipo di firma (autografa e/o digitale) e non da ultimo lo specifico tipo di PEC (CEC-PEC, PEC semplice, PEC ID). Anche a questo riguardo se da una parte, soprattutto quando l'invio è effettuato tramite PEC non ID (per capirci ad esempio la ormai

---

<sup>7</sup> L'art. 47 CAD pone un vero e proprio obbligo di utilizzo degli strumenti telematici nelle comunicazioni tra le Pubbliche Amministrazioni e prevede che l'inosservanza delle disposizioni di cui all'art. 47, comporti responsabilità dirigenziale e disciplinare (art. 47, comma 1-bis).

soppressa CEC-PEC), appare necessaria la firma degli allegati considerato che la firma digitale può essere “surrogata” solo da PEC-ID ovvero da una PEC rilasciata con particolari procedure di riconoscimento del titolare, dall’altra i giudici, prima del TAR pugliese e poi del Consiglio di Stato, hanno deliberato invece che a fronte di particolari condizioni in cui sia possibile identificare con esattezza il mittente debba essere ritenuto valido il contenuto della PEC medesima (comunicazione e allegati) e che quindi gli allegati (generalmente il “cuore” della comunicazione via PEC) non debbano necessariamente essere firmati digitalmente (TAR Puglia 6 agosto 2014 n 11030) (vedi per una analisi più approfondita il capitolo “Sentenze esemplari”)

L’orientamento giurisprudenziale sembra dunque andare nella direzione di cogliere per così dire “la sostanza” della questione e considerare valide istanze che apparivano ai giudici, in qualche modo, come per altro esplicitato nelle sentenze, solo formalmente incomplete. Tuttavia, se in comunicazioni tra organismi della PA questa posizione “non formalista” può avere un suo senso tenuto conto del fatto che quasi sempre appare semplice attribuire la corretta paternità ad un documento, almeno nel senso della attribuzione ad una precisa istanza della PA, e anzi tale posizione potrebbe essere condivisibile soprattutto nell’ottica di una velocizzazione e semplificazione dei rapporti, ben diverso è il caso quando risultano coinvolti soggetti privati, siano essi cittadini o imprese. Rimane fermo che sarebbe sempre auspicabile una correttezza anche formale in tutti i procedimenti della PA, proprio per non costringere i giudici ad interpretazioni “troppo libere” della normativa.

### **Identificazione e sottoscrizione**

La attuale fase di transizione dal cartaceo al digitale all’interno della PA e nei rapporti tra PA e cittadini e/o imprese sta comportando un lavoro burocratico ed uno sforzo normativo non indifferente: da una parte la necessità di recepire le indicazioni europee, dall’altra il tentativo di “cavalcare” (o quanto meno di non farsi lasciare troppo indietro) le possibilità effettivamente offerte dalla informatizzazione dei sistemi e delle organizzazioni complesse (quali sono gli uffici della PA) portano ad un continuo aggiustamento della normativa senza che

sia ben chiaro il fine ultimo. Ciò ha portato gli uffici pubblici (sia quelli centrali che quelli periferici come ad esempio le scuole) a un iper-lavoro e ad un cambiamento continuo nelle procedure da adottare senza, almeno per ora, un effettivo beneficio né per gli uffici né per i cittadini ai quali sfuggono i vantaggi dell'utilizzo di una PEC piuttosto che di una raccomandata A/R o la necessità di apporre una firma digitale ad un documento inviato alla PA.

In particolare per quanto riguarda l'oggetto di questo lavoro, ciò su cui sembra necessario appuntare l'attenzione per dipanare la questione dei collegamenti tra PEC FD e MT è legata all'identificazione degli assegnatari di PEC da parte del gestore del servizio di posta elettronica certificata, dato che la normativa sulla PEC (DPR 68/2005 e regole tecniche) non specifica nulla a riguardo. La PEC è nata come strumento di trasmissione di documenti (che possono essere effettivamente attribuiti ad un soggetto in base alla Firma Digitale e collocati in un tempo preciso tramite la Marca Temporale) e dato il suo uso ormai pressoché in tutti i procedimenti amministrativi, dovrebbe forse diventare essa stessa mezzo di identificazione e sottoscrizione, concetti in realtà distinti tra loro. Occorre probabilmente ripensare dall'inizio le norme tecniche per dare una coesione e una coerenza definitive al sistema PEC, FD, MT.

Non va dimenticato infine che la PEC è stata posta fino a poco tempo fa come la “chiave di volta” del processo di sburocratizzazione della PA, probabilmente operando quel processo di sovrapposizione tra strumento di trasmissione e identificazione dell’assegnatario di cui abbiamo appena detto; solo nell’ultimissimo periodo si è proceduto ad una approfondita analisi della questione dando finalmente attuazione al concetto di identificazione elettronica attraverso un mezzo diverso, quello della Identità Digitale (sistema Pubblico per la gestione dell’Identità Digitale SPID) con il quale le pubbliche amministrazioni potranno consentire l’accesso in rete ai propri servizi (oltre che con lo stesso SPID si potrà accedere a tali servizi anche mediante la carta d’identità elettronica e la carta nazionale dei servizi (il termine entro il quale la disposizione entrerà in vigore sarà stabilito con il relativo decreto attuativo), iniziando effettivamente ed efficacemente a distinguere tra identità digitale, mezzo di trasmissione e documenti informatici effettivamente attribuibili ad un soggetto.

In sostanza l'identità digitale SPID è rilasciata dai Gestori di Identità Digitale (Identity Provider), ovvero soggetti privati accreditati da AgID (Agenzia per l'Italia Digitale) che, nel rispetto delle regole emesse dall'Agenzia, forniscono le identità digitali e gestiscono l'autenticazione degli utenti. Per ottenere un'identità SPID l'utente deve farne richiesta al gestore, il quale, dopo aver verificato i dati del richiedente (qui è l'elemento dirimente, in quanto il gestore è tenuto per legge a verificare i dati del richiedente, cosa che non avviene nel caso della PEC, emette l'identità digitale rilasciando le credenziali all'utente. Va detto, come sarà precisato meglio più oltre, che diversi provvedimenti recenti, ad esempio quelli riguardanti il Processo Amministrativo Telematico o le aste telematiche richiedono per le caselle di PEC utilizzate in quei provvedimenti, specifiche tali per cui l'identificazione del “proprietario” di casella diventa di fatto obbligatoria, ma l'introduzione di questo elemento non avviene nella normativa generale, ma in provvedimenti applicativi riferiti ad ambiti specifici e particolari, il che più che chiarezza ingenera confusione.

## NORMATIVA DI RIFERIMENTO

Prima di entrare nella trattazione specifica appare opportuno elencare la normativa di riferimento anche per chiarire termini e concetti che verranno usati successivamente. Necessaria premessa è che ci troviamo in un periodo di transizione, nel quale le norme vengono frequentemente aggiornate.

La PEC e gli altri strumenti informatici qui trattati infatti sono oggetto di diversi atti legislativi e regolamentari che prendono le mosse dai primi tentativi di digitalizzazione della PA e che sono stati modificati e integrati successivamente in modo anche sostanziale. Spesso questi strumenti vengono trattati all'interno di provvedimenti di portata molto più vasta (leggi quadro, leggi di stabilità, “salva Italia” etc.) per cui diventa molto difficile andare a cercare il singolo comma, che magari sostituisce un solo termine, all'interno di provvedimenti spesso composti da centinaia di articoli e non risulta ragionevole proporre come normativa di riferimento provvedimenti nati per scopi anche molto lontani dagli argomenti di

cui qui trattiamo. In sostanza, come talvolta purtroppo accade per argomenti considerati rilevanti solo dal punto di vista tecnico, ciò che è mancato è uno sguardo d'insieme in grado di vedere al di là del singolo provvedimento e anche, va detto, dei vari interessi coinvolti (basta pensare al fatto che la PEC, dopo il tramonto della CEC PEC, è rilasciata da imprese private, alle quali si paga un canone annuale, per capire come le scelte tecniche siano spesso imposte e mediate anche da interessi economici)

L'elenco che segue pertanto riguarda le disposizioni più recenti che formano un insieme di norme abbastanza coerente e completo e che risultano essere rilevanti in modo significativo rispetto all'oggetto di questo lavoro.

Va notato che in questo campo, oltre alle specifiche norme, assumono particolare rilevanza le cosiddette “Norme tecniche” emesse tramite Regolamenti e Decreti successivi, spesso anche a distanza di anni dalla norma originaria. Risultano poi nella applicazione pratica molto importanti le circolari ministeriali e quelle di enti e istanze della PA molto differenti tra loro.<sup>8</sup> Si tratta, in genere, di iniziative ovviamente meritorie che mettono in grado il cittadino o l'impresa di operare correttamente. Tuttavia non potendo escludere a priori anche in queste circolari applicative errori o imprecisioni (da cui quasi sempre le varie agenzie si cautelano ribadendo che l'unica fonte normativa valida è quella ufficiale) potrebbero esse stesse diventare sorgente di contenzioso (d'altra parte accade che quasi in ogni circolare o decreto venga ripetuto cosa è un documento informatico o cosa è la firma elettronica e i vari tipi che di essa esistono, e ciò appare quantomeno ridondante, ma basta questo a far capire che la normativa sottostante non è di una chiarezza esemplare se appunto ogni ente sente la necessità di far chiarezza, probabilmente a se stesso prima che a cittadini e imprese).

Tutta la normativa in merito prende l'avvio dalla direttiva comunitaria 1999/93/CE, la quale ha imposto ai vari stati membri un progressivo aggiornamento e una progressiva digitalizzazione e informatizzazione delle procedure tra PA e PA e tra PA, cittadini e imprese. La suddetta direttiva è stata superata da un nuovo regolamento comunitario (il cosiddetto eIDAS)

---

<sup>8</sup> Sull'analisi del modo di legiferare in questo campo e del ruolo che assumono circolari o pareri dei vari enti vedi più avanti

immediatamente operativo che pone obiettivi ancora più ambiziosi a tutti gli stati membri, introducendo un quadro di riferimento valido per tutti i paesi della Comunità Europea. Considerando che sulla base della direttiva citata, ed oggi abrogata, sono state emanate normative per più di 15 anni, è ovvio che il nuovo Regolamento Comunitario in materia renderà necessario un accurato lavoro di revisione e modifica (in gran parte già iniziato) della normativa esistente per renderla conforme al nuovo Regolamento.

Per quanto riguarda la normativa nazionale, senza andare troppo indietro nel tempo e pur considerando che sono applicabili tutte le normative precedenti in materia di notifica, di sottoscrizione e di efficacia probatoria dei vari tipi di documento, anche se non fanno diretto riferimento agli strumenti elettronici, si può prendere avvio, nella enumerazione delle fonti normative dall'art.27 della [Legge 16 gennaio 2003, n.3](#) (“Disposizioni ordinamentali in materia di pubblica amministrazione”) e dall’articolo 10 della [Legge n. 229 del 29 luglio 2003](#), cosiddetta “legge di semplificazione 2001”.

Nella prima delle due citate leggi, al comma 8 del suddetto articolo 27 vengono elencati per la prima volta in maniera chiara gli obiettivi che il governo persegue in materia di informatizzazione, dematerializzazione e comunicazione informatizzata tra PA e cittadini e imprese; si parla di diffusione delle firme elettroniche, di estensione dell'utilizzo della posta elettronica, di ricorso a procedure telematiche da parte della PA. Si dà insomma l'avvio al processo di trasformazione della burocrazia della macchina dello stato da cartacea ad informatizzata.

All'interno dell'articolo 10 della citata legge di semplificazione 2001 si procedette ulteriormente a dare effettiva delega al governo per il riassetto in vari settori della PA con lo scopo dichiarato di favorire lo snellimento delle procedure amministrative. Vale la pena sottolineare che già allora venivano sostanzialmente poste due questioni, una di carattere tecnico/amministrativo e una di carattere politico.

La prima, desumibile da diversi commi dello stesso articolo 27 Legge 16 gennaio 2003, n.3, si può riassumere nel fatto di voler assicurare tutte le specifiche

tecniche che garantissero la possibilità di attribuire al documento informatico, alla firma digitale e a tutti gli altri strumenti informatici utili ad una effettiva dematerializzazione e informatizzazione della PA, la capacità di potersi sostituire all’analogo documento cartaceo, alla firma olografa e alla raccomandata A/R garantendo sicurezza, privacy e al tempo stesso permettendo di assegnare agli strumenti informatici un valore legale e probatorio.

La seconda invece la ritroviamo nel comma b) dell’articolo 10 ed enuclea lo scopo politico della dematerializzazione degli uffici della PA e dei rapporti tra cittadini, imprese e la stessa PA. Si trattava infatti di: “*rivedere la disciplina vigente al fine precipuo di garantire la più ampia disponibilità di servizi resi per via telematica dalle pubbliche amministrazioni e dagli altri soggetti pubblici e di assicurare ai cittadini e alle imprese l’accesso a tali servizi secondo il criterio della massima semplificazione degli strumenti e delle procedure necessari e nel rispetto dei principi di egualanza, non discriminazione e della normativa sulla riservatezza dei dati personali*”<sup>9</sup>.

Ad oggi possiamo dire che numerosi passi in avanti sono stati compiuti in entrambe le questioni, sebbene risulti ancora prematuro parlare di un processo pienamente compiuto e soprattutto della cui portata siano pienamente coscienti cittadini, imprese e uffici della PA.

Tra le norme più rilevanti ai nostri scopi vanno citate:

[Decreto del Presidente della Repubblica dell’11 febbraio 2005, n. 68](#) e i collegati documenti tecnici (decreto ministeriale del 2 novembre 2005 rubricato “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata (G.U. del 14 novembre 2005, n. 265) e Circolare CNIPA del 24 novembre 2005, n. 49):

definiscono le modalità di funzionamento del sistema informatico tramite il quale si realizza la PEC e che garantiscono la effettiva interoperabilità tra i diversi gestori di posta certificata, definendo quindi le le caratteristiche di sicurezza e di certificazione della trasmissione che rendono i messaggi opponibili a terzi.

---

<sup>9</sup> Comma b) art. 10.(Riassetto in materia di società dell’informazione) . Legge 29 luglio 2003, n. 229

DECRETO LEGISLATIVO 7 marzo 2005, n. 82 e successive modifiche e integrazioni, cosiddetto Codice dell'amministrazione digitale (CAD).

Si tratta della "madre di tutte le norme" per l'informatizzazione della PA e dei suoi rapporti con i cittadini e le imprese, alla quale si fa riferimento in tutta la normativa successiva. Si tratta di un decreto che ha subito dalla sua approvazione fino ad oggi almeno un centinaio di aggiornamenti e modifiche di cui almeno 6 modifiche sostanziali alla struttura del documento e almeno 4 circolari esplicative. E' il principale riferimento per la digitalizzazione della PA e delle imprese private. Le modifiche più significative al CAD sono state, in ordine cronologico: DL 4 aprile 2006 n. 159, DL 185 /2008 convertito in Legge n. 2/2009, Legge 18 giugno 2009 n. 69, Legge 3 agosto 2009 n. 102, DL 30 dicembre 2010 n. 235 (che modifica ben 53 articoli su 92 e ne introduce altri 9 operando una modifica strutturale del CAD tanto che in quell'occasione si parlò di nuovo CAD), il DL 18 ottobre 2012 n. 179 convertito con modificazioni dalla Legge 221/2012, Legge 23 dicembre 2014 n. 190. L'elenco completo degli aggiornamenti e delle circolari e la versione vigente del CAD è disponibile sul sito Normattiva<sup>10</sup>

In particolare, con riferimento a quanto oggetto di questo lavoro il CAD, oltre a contenere tutte le definizioni dei termini riguardanti gli strumenti elettronici qui analizzati, dalla firma elettronica, alla validazione temporale, afferma che:

- i. il CAD si applica alla PA e alle società a controllo pubblico;
- ii. i cittadini e le imprese hanno il diritto all'uso delle tecnologie telematiche;
- iii. il mezzo telematico è il mezzo esclusivo della comunicazione tra imprese e PA;
- iv. il documento informatico ha validità ed efficacia probatoria e in questa funzione riveste particolare importanza la firma elettronica;
- v. la PEC è lo strumento da utilizzare per le comunicazioni elettroniche nel caso in cui servano le ricevute di invio e di consegna (come la raccomandata AR);

---

<sup>10</sup><http://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2005-05-16&atto.codiceRedazionale=005G0104&currentPage=1>

- vi. le amministrazioni pubbliche devono pubblicare un indirizzo di PEC cui il cittadino possa rivolgersi per qualsiasi richiesta.

LEGGE 28 gennaio 2009, n. 2 - Conversione in legge, con modificazioni, del [Decreto legge 29 novembre 2008](#), n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale, cosiddetto provvedimento “anti crisi” che contiene modifiche al Codice dell’Amministrazione Digitale e al Regolamento per l’utilizzo della Posta elettronica.

I commi 6,7,8 e 9 dell’art. 16 sanciscono che:

- i. le società esistenti sono tenute a dichiarare il proprio indirizzo PEC al Registro delle Imprese entro il 2011;
- ii. le società di nuova costituzione lo devono dichiarare al momento della costituzione;
- iii. i singoli enti che compongono la PA devono dichiarare il proprio indirizzo PEC.

[Decreto Presidente del Consiglio dei Ministri del 6 maggio 2009 \(G.U. 25 maggio 2009, n.119\)](#) recante Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini.

Definisce le modalità con cui ciascun cittadino può richiedere ed ottenere gratuitamente il rilascio di una PEC dal dipartimento per l’innovazione e le tecnologie della Presidenza del Consiglio dei Ministri ed è la norma che ha consentito la nascita della CEC- PAC, progetto poi abbandonato.

[DECRETO LEGGE n. 179 del 2012](#) introduce ulteriori novità in merito alla PEC, si istituisce un indice nazionale degli indirizzi PEC delle imprese e dei professionisti e si obbligano anche le imprese individuali a dotarsi di un indirizzo PEC con lo scopo di favorire e velocizzare le comunicazioni con la PA.

La Legge di stabilità del 2012<sup>11</sup> è intervenuta sul Codice di procedura civile introducendo l'utilizzo obbligatorio della PEC:

l'art. 25 (non a caso rubricato “Impiego della posta elettronica certificata nel processo civile”) introduce diverse modifiche al C.p.C. che tendono a rendere pienamente operativo l’uso della PEC nel processo civile stabilendo tra l’altro l’obbligo per il difensore di indicare negli atti di parte l’indirizzo di PEC comunicato all’Ordine così da consentire una modalità semplice di notificazione.

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 del DECRETO LEGISLATIVO 7 marzo 2005, n. 82 e successive modifiche e integrazioni - Codice dell'amministrazione digitale

Si tratta del decreto attuativo del **CAD** in base alle modifiche introdotte dal decreto legislativo n. 235 del 2010 sulle modalità di sottoscrizione di un documento informatico mediante firma elettronica e digitale. L’obiettivo è modernizzare i rapporti tra amministrazione e imprese aumentando le tipologie di firme elettroniche che è possibile utilizzare, portando ad una sostanziale e piena equiparazione con il documento cartaceo. Va notato come siano passati ben 3 anni tra l’emanazione di queste regole tecniche e la norma che le prevedeva

Va poi citato il REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 (EIDAS) Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (Gazzetta Ufficiale dell’Unione Europea L 257 del 28 agosto 2014)

A questo Regolamento sono connessi i Regolamenti di esecuzione dell’8 settembre 2015 numero 1501, 1502, 1505 e 1506. Ai fini del nostro lavoro risulta rilevante in particolare l’ultimo ovvero il Regolamento di esecuzione (UE) 2015/1506 della Commissione, dell’8 settembre 2015 ovvero il regolamento che

---

<sup>11</sup> LEGGE 12 novembre 2011, n. 183; Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (Legge di stabilità 2012). (11G0234) (GU n.265 del 14-11-2011 - Suppl. Ordinario n. 234 )

stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

L'impatto del Regolamento eIDAS sulla normativa vigente sarà analizzato in un apposito capitolo.

Infine non si può trascurare il fatto che è stato approvato uno Schema di Decreto Legislativo recante modifiche e integrazioni al Codice dell'Amministrazione Digitale, che pur non essendo ancora in vigore, lo sarà sicuramente dal luglio 2016 (in concomitanza con l'entrata in vigore di eIDAS) e apporta modifiche di rilevanza tale che si può parlare a buon diritto di nuovo CAD e quindi, anche mettendo in conto la possibilità di eventuali modifiche prima della sua emanazione, non si può non citarlo in questa analisi.

Le modifiche apportate al CAD dal citato schema di Decreto Legislativo saranno oggetto di un apposito capitolo.

### **Considerazioni in merito al modo di normare**

Si vuole qui analizzare il modo di normare, in particolare l'uso della legislazione delegata, la emissione di norme tecniche, sia a livello centrale (leggi, DPCM) sia da parte di diverse istanze della PA (Corte dei Conti, Cassazione), l'uso massiccio di Circolari ed altri atti di natura esplicativa, ma talvolta anche prescrittiva. Si tratta di una analisi sommaria ma che ben mette in evidenza la complessità di un modo di legiferare e normare che se talvolta presenta indubbi vantaggi può anche nascondere diverse insidie.

### **Il caso particolare dei documenti classificati**

Riportiamo qui brevemente alcune osservazioni su un'area di interesse estremamente specifico ma che appare interessante non tanto riguardo alla normativa in sé quanto alla complessità del modo attraverso cui si arriva alle norme. Ci riferiamo al problema della firma elettronica sui documenti cosiddetti classificati ovvero quei documenti cui “è stata apposta una classifica di segretezza

in conformità a quanto stabilito dalle vigenti norme in materia di protezione e tutela delle informazioni classificate". Il DPCM del 6 novembre 2015, richiama sia il CAD (D. Lgs. 82/2005) sia DPCM 22 febbraio 2013, e individua le Regole tecniche per l'emissione, la gestione e l'utilizzo dei certificati qualificati necessari per la sottoscrizione digitale dei documenti classificati. Il problema è che il decreto stabilisce che ai documenti si potrà applicare quanto previsto dall'art. 20 del CAD in relazione alla loro validità e rilevanza agli effetti di legge solo se tali documenti saranno formati secondo quanto previsto da una specifica Direttiva e dal Disciplinare tecnico, ma sia la Direttiva sia il Disciplinare Tecnico non esistono ancora e dovranno essere emanati (peraltro in base all'art. 33 del DPCM di cui si parla) Riguardo alla Direttiva (già prevista da un DPCM del 2011 e ancora non emanata per chissà quali motivi) essa dovrebbe essere approvata entro 12 mesi dall'adozione del DPCM 6 novembre 2015. Il Disciplinare Tecnico, dovrà essere emanato insieme a un Manuale Operativo, riguardante disciplina e procedure dell'Autorità di Certificazione speciale che si occuperà del rilasci di certificati e firme necessarie allo specifico scopo di validare i documenti classificati.

Come si vede di nuovo un rimando a Regole tecniche di là da venire che peraltro dovrebbero in questo caso anche tenere conto di "ulteriori accordi internazionali di settore" e quindi probabilmente piuttosto complesse. Nel frattempo? Nel frattempo anche se il DPCM è nuovo "continuano a trovare applicazione le direttive emanate dall'Autorità nazionale per la sicurezza ai sensi e per gli effetti dell'articolo 50, comma 1, del decreto del Presidente del Consiglio dei Ministri 3 febbraio 2006, recante «Norme unificate per la protezione e la tutela delle informazioni classificate», pubblicato nella Gazzetta Ufficiale - Serie generale, n. 46 del 24 febbraio 2006" con una commistione tra regole nuove e vecchie che con tutta probabilità non aiuterà gli operatori del settore a svolgere al meglio il loro lavoro. Per una volta tanto, magari anche considerando la delicatezza della questione di cui si sta trattando, forse si poteva fare in modo da emanare insieme Norme Generali e Regole Tecniche.

## **Legislazione delegata: pregi e limiti**

E' noto come da tempo sia invalsa, a livello legislativo, l'abitudine a ricorrere alla "legislazione delegata". Si tratta del fatto che il Parlamento approva una legge con prescrizioni di carattere generale riguardanti un certo ambito che contiene una delega che rimanda a successivi decreti del Governo la pratica attuazione di quanto stabilito in linea generale nella legge approvata dal Parlamento. Questa prassi trova conferma già nella Costituzione ma pone diversi problemi che anche la Corte Costituzionale ha affrontato in diverse occasioni<sup>12</sup> rilevando come la prassi parlamentare abbia modificato in modo sostanziale questo modo di legiferare estendendone in modo significativo la portata.

L'istituto era stato pensato essenzialmente per essere usato in situazioni particolari come l'emanazione di Decreti Delegati per riordinare una materia ampia e volti a costituire una sorta di Testo Unico in ambiti in cui la sovrapposizione di norme nel tempo aveva creato situazioni difficili da gestire con una legge ordinaria (ad esempio i Decreti Delegati sulla Pubblica Istruzione<sup>13</sup> che sono stati alla base della normativa scolastica per alcune decine di anni senza modifiche sostanziali).

Oggi, per motivi diversi, ma di natura più politica che giuridica e sui quali non è il caso qui di soffermarsi, si tende secondo molti giuristi ad abusare di questo strumento, spesso adducendo come motivo la complessità tecnica, come nel caso della legislazione riguardante il processo complessivo della digitalizzazione della pubblica amministrazione, o talvolta, la sostanziale "neutralità tecnica" dei decreti attuativi una volta che la legge delega sia "ben fatta". Il risultato pratico è che spesso la legislazione delegata sfugge al controllo del Parlamento (prima della promulgazione sono previsti i pareri delle Commissioni parlamentari competenti ma tali pareri non sono vincolanti per il governo) e spesso viene costruita senza il necessario raccordo con le istanze che nella famosa "società civile" si sono formate per gestire le innovazioni tecniche ed economiche che necessariamente devono essere il sostegno per ogni riforma legislativa che aspiri ad essere efficace.

---

<sup>12</sup> Si veda ad esempio <http://www.cortecostituzionale.it/documenti>

<sup>13</sup> Di tratta di una legge delega e di 5 DPR emanati nel 1973

Il ricorso eccessivo alla legislazione delegata è ampiamente criticato da più parti<sup>14</sup>. Si tratta come si è detto di un problema politico assai più che giuridico e si inquadra nella tendenza a investire il Governo di poteri sempre più forti e ad allentare i controlli del Parlamento sul Governo. Che la situazione attuale sia il risultato di un profondo cambiamento politico è ben espresso nell'articolo citato dove si ricorda come nel 1992, ..”con una svalutazione galoppante e la lira fuori dallo Sme, il governo Amato chiese 4 maxideleghe su pensioni, sanità, pubblico impiego, enti locali. Il presidente Scalfaro si dichiarò contrario ai pieni poteri dell'esecutivo, il presidente della Camera (Giorgio Napolitano) idem..”.

Qui non si vuole fare una analisi approfondita di risvolti politici della questione né criticare l'uso della legislazione delegata, ma si vuole solo far notare come il ricorso pressoché esclusivo alla legislazione delegata nel campo della informatizzazione della PA e dei rapporti tra PA e cittadini e imprese, se da una parte permette una certa tempestività nelle decisioni, dall'altra rischia di rinchiudere il Governo in una sorta di autoreferenzialità tecnica che non sempre è il modo migliore per affrontare temi che non sono solo ed esclusivamente tecnici.

Va pure ribadito che i vantaggi di velocità nella emanazione di legislazione delegata sono nella quasi totalità dei casi vanificati dai tempi lunghissimi (in alcuni casi diversi anni) che passano dalla approvazione della norma alla emanazione delle relative Regole tecniche.

### **Le Regole tecniche: pro e contro**

Il mero elenco di tutte le norme, riferite al CAD e alla sua pratica implementazione, che recano nel titolo la dicitura “Regole tecniche” riempirebbe diverse pagine. Non solo ma le Regole Tecniche provengono da DPR, DPCM, Decreti dei vari Ministeri, Decreti di istanze varie della PA.

Ora, è evidente che in una materia dai risvolti tecnici molto complessi e in rapidissima evoluzione tecnologica è assolutamente necessario distinguere tra una normativa generale di riferimento e le relative regole tecniche per implementarla praticamente. Tuttavia desta perplessità il numero elevato di tali Regole tecniche e

---

<sup>14</sup> Si veda per tutti l'articolo (non recentissimo ma sempre valido) di Michele Ainis sull'Espresso all'indirizzo: <http://espresso.repubblica.it/opinioni/legge-e-liberta>

il fatto che nella quasi totalità dei casi esse sono stabilite con norme di rango elevato, quali DPR o DPCM che in quanto tali avranno bisogno per la loro modifica di norme di rango altrettanto elevato (e presumibilmente di complessa e lenta preparazione ed emanazione). Tutto ciò non pare accordarsi troppo bene con la logica per cui le Regole tecniche vengono separate dalla normativa di base proprio allo scopo di permetterne un rapido adeguamento in caso di necessità. Per questo molti addetti ai lavori ritengono ad esempio che sarebbe più vantaggioso operare in modo più snello, demandando le regole tecniche non a norme di legge ma a disposizioni di organi tecnici.

Si tratta di una opinione non priva di una sua logica ma si scontra con diverse difficoltà: anzitutto organismi tecnici in grado di intervenire con competenza e rapidità in questo campo al momento non ci sono (l'AgID<sup>15</sup> sembra il naturale destinatario di questo compito ma andrebbe opportunamente potenziato e ridefinito nella struttura e nei compiti), poi va detto che le Regole tecniche tanto neutre non sono dato che gli strumenti informatici di cui stiamo parlando sono disponibili per cittadini e imprese solo a pagamento e quindi l'adozione di specifiche tecniche di un tipo o dell'altro possono influire sul mercato e condizionarne lo sviluppo.

Il riferimento normativo di base, dal quale deriva la possibilità (e la necessità) di emanare Regole tecniche nel campo oggetto di studio, è l'art. 71 del CAD che recita al comma 1 nella sua nuova presumibile<sup>16</sup> versione: “*Con decreto del Ministro delegato per la semplificazione e la pubblica amministrazione, su proposta dell'Agid, di concerto con il Ministro della giustizia e con i Ministri competenti, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e il Garante per la protezione dei dati personali nelle materie di competenza, sono adottate le regole tecniche per l'attuazione del presente Codice.*” Si tratta, da quello che si può capire di un passo

---

<sup>15</sup> Già nella storia dei nomi che questa Agenzia ha assunto nel tempo , prima CNIPA, poi DigitPA ora AgID sono visibili i tentativi di renderla idonea a svolgere con efficacia i compiti che le sono assegnati. Il cambiamento di nome infatti è sempre coinciso con una ridefinizione dei compiti e anche oggi, pur mantenendo inalterato il nome, lo SCHEMA DL 20/01/2016 ne ridisegna radicalmente struttura e mansioni

<sup>16</sup> Presumibile in quanto è la versione contenuta nello Schema di decreto di modifica del CAD approvato dal Consiglio dei Ministri il 20 gennaio 2016

avanti notevole perché pare configurare un unico decreto di Regole tecniche, anche se resta da capire se questa sarà davvero l'interpretazione che verrà data a questo articolo e che fine farebbero le innumerevoli Regole tecniche già emanate. A questo proposito la nuova formulazione del CAD introduce qualche ulteriore dubbio dato che viene anche cancellato il fatto che le regole tecniche pre-vigenti restano fino ad entrata in vigore delle nuove<sup>17</sup>. Questa cancellazione sembra prefigurare un pericolosissimo periodo di “interregno” letteralmente senza regole il che appare davvero senza senso per cui con tutta probabilità, considerato che le nuove regole, che dovrebbero, a rigore, arrivare prima del 1 luglio 2016, non saranno sicuramente pronte per quella data, la norma sarà corretta nella versione definitiva (o almeno così tutti sperano che avvenga).

D'altra parte va considerato che esiste in Italia un problema di autonomia normativa dei vari settori dell'amministrazione, in genere molto gelosi di questa autonomia e se questo atteggiamento affonda le sue radici nella storia italiana, a molti sembra poco efficace e foriero di possibili conflitti e contraddizioni il fatto che istanze diverse di fatto si trovano a normare la stessa questione.

Non solo, ma le stesse Regole tecniche vengono modificate o integrate in tempi rapidissimi e innumerevoli volte sicché risulta davvero poco agevole stare “*al passo*”.

Così si può fare l'esempio dei decreti del Ministero della Giustizia che ha emanato in successione il [DECRETO 21 febbraio 2011, n. 44](#) “*Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82*”, poi dopo un anno il [DECRETO 15 ottobre 2012, n. 209](#) “*Regolamento recante: «Regole tecniche per l'adozione nel processo civile e penale delle tecnologie dell'informazione e comunicazione»*”, poi ancora dopo un anno il [DECRETO 3 aprile 2013, n. 48](#) “*Regolamento recante modifiche al D.M. n. 44/2011, concernente le regole tecniche per l'adozione nel processo civile e nel processo*

---

<sup>17</sup>Il comma 2 dell'art.71 del CAD nella formulazione vigente recita: “*Le regole tecniche vigenti nelle materie del presente codice restano in vigore fino all'adozione delle regole tecniche adottate ai sensi del presente articolo*” e questa frase è quella cancellata nel nuovo CAD

*penale delle tecnologie dell'informazione e della comunicazione”* e qui ci fermiamo non perché non vi siano altre e più recenti Regole Tecniche ma perché è sufficiente per capire che è difficile per tutti lavorare serenamente se con cadenza annuale si modificano norme che anche se si chiamano Regole tecniche hanno una incidenza rilevantissima sul cuore dell’ordinamento giudiziario di cui il processo penale e civile costituiscono la massima espressione.

Per un esempio di come le Regole tecniche possano creare problemi interpretativi e portare a situazioni non chiare riportiamo il caso della Corte dei Conti.

Nella Gazzetta Ufficiale n. 256 del 3 novembre 2015, è stato pubblicato il [decreto della Corte dei Conti del 21 ottobre 2015](#) con il quale sono state rese note le prime regole tecniche ed operative per l'utilizzo della posta elettronica certificata nei giudizi dinanzi alla Corte dei conti, incluse le comunicazioni e notificazioni e il deposito di atti o documenti. Questo decreto prevede, e non poteva essere diversamente, che, per quanto non previsto dal decreto, restano ferme le disposizioni sul processo civile e quelle della legge 21 gennaio 1994, n. 53, in quanto siano applicabili e non siano modificate dalle disposizioni speciali sui giudizi dinanzi alla Corte dei Conti .

Quello che qui interessa, al di là delle specifiche sulle date di validità o altri dettagli, è che il decreto disponga che tutte le comunicazioni e notificazioni a cura delle Segreterie delle Sezioni giurisdizionali della Corte dei conti sono effettuate esclusivamente per via telematica tramite PEC

Fin qui “tutto bene”, a parte la classica dicitura in quanto siano applicabili che anche se doverosa introduce già un margine di incertezza; quello che non è chiaro è però perché si sia sentita la necessità di introdurre un art. 7 che testualmente recita “*Requisiti della casella di posta elettronica certificata 1. Le caselle di posta elettronica certificata indicate facoltativamente come domicilio, ai sensi dell'art. 8 del presente decreto, o comunque utilizzate nei rapporti con le Sezioni giurisdizionali e le Procure della Corte dei conti devono essere dotate di idonei sistemi di protezione dall'invio di messaggi indesiderati e da eventuali altre minacce informatiche e devono possedere i requisiti dimensionali e tecnici minimali stabiliti con le istruzioni di cui all'art. 10.”*

Qui non solo si introduce una norma che rimanda ad ulteriori specifiche da emanarsi anche ripetutamente in tempi successivi ma si vanno a specificare caratteristiche tecniche della PEC che sono disciplinate altrove, in normative di carattere più generale. Di nuovo si introduce un elemento di scarsa chiarezza dato che se ne potrebbe dedurre che caselle di PEC idonee in un altro tipo di processo non lo sono nei processi davanti alla Corte dei Conti. E poi a chi spetta stabilire se quella particolare PEC è “buona” o no? Non è sufficiente che si tratti di PEC e perciò in quanto tale, conforme alle normative di carattere generale (oggi addirittura con l’introduzione di eIDAS, sovranazionali), idonea a tutti gli usi cui la PEC sia riconosciuta? Se passa il principio che ogni istanza che preveda l’uso della PEC può aggiungere (e magari togliere) qualche caratteristica tecnica non si introducono elementi di incertezza che possono rendere problematico l’uso dello strumento telematico?

### **Le Circolari: uso e abuso**

Un discorso simile a quello fatto per le Regole tecniche si può fare a proposito delle Circolari. Praticamente ogni istanza della PA, centrale o periferica che sia, emana circolari..

E’ noto peraltro che esiste una diffidenza di vedute sul valore delle circolari come sottolinea esplicitamente anche il Consiglio di Stato, Adunanza Plenaria, [sentenza 14.11.2011, n. 19](#) che afferma: “*Quanto alla questione della rilevanza delle circolari, è nota la varietà delle opinioni dottrinarie e giurisprudenziali sulla natura di questi atti e sulla loro impugnazione, varietà dovuta peraltro alla molteplicità delle fattispecie che vengono riunite sotto quest’unica denominazione come riconosce esplicitamente l’articolo 26 della legge n. 241 del 1990*”.

Non è questa la sede per un’approfondita disamina del valore giuridico delle circolari e della relativa giurisprudenza.

Qui vogliamo ancora sottolineare che se le Circolari, nel campo oggetto di studio, non si limitano ad illustrare la normativa e a dare indicazioni su come applicarla nel modo più corretto e conveniente, ma introducono elementi anche solo minimamente non conformi alla norma sottostante, possono introdurre ulteriori elementi di confusione. In particolare nel caso della PEC e della FE, l’importanza

delle circolari deriva proprio dal loro ruolo interpretativo nell'utilizzo pratico dello strumento informatico oltre a quello di dirimere i dubbi sulle definizioni ( si pensi ai diversi tipi di firma) , assumendo de facto, il ruolo di “ausilio giuridico” sebbene non rivesta alcuna rilevanza ufficiale per il Giudice eventualmente chiamato a verificare la legittimità dell'atto che può però valutare l'effetto che l'utilizzo della circolare può avere indotto nell'utilizzatore.

Ad esempio la circolare n. [3 del 2014 della Ragioneria dello Stato](#) è un buon esempio di una circolare esplicativa che indubbiamente chiarisce alcuni aspetti riguardo alla accettabilità della documentazione trasmessa in sede di controllo di regolarità amministrativa e contabile e può aiutare gli uffici a svolgere in modo efficace il loro lavoro. Tuttavia c'è da chiedersi: c'era proprio bisogno di riportare le definizioni di firma elettronica o documento digitale già presenti nel CAD? Oggi che tali definizioni sono per la quasi totalità eliminate dal CAD e fanno riferimento a quanto definito in eIDAS, cosa accade alla nostra circolare? Rimane ancora valida o le nuove definizioni possono inficiare le deduzioni e le prescrizioni della Ragioneria dello Stato?

## LA PEC

### Brevissima storia

La PEC è disciplinata principalmente dal D.P.R. 11.2.2005, n. 68 : "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, e dalle regole tecniche contenute nel relativo D.M. 2.11.2005, recante appunto "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata". Queste norme sono da coordinare con quelle contenute nel CAD e nelle molteplici successive modifiche allo stesso. Infine esistono diverse norme settoriali che, emanate dai diversi ministeri o da diverse istanze disciplinano l'uso della PEC in procedimenti particolari (Processo Telematico nelle sue varie articolazioni, Aste giudiziarie telematiche etc.)

In particolare il CAD disciplina la PEC e all'art. 48 comma 2 dispone che "*la trasmissione del documento informatico per via telematica, [...] equivale, [...] alla notificazione per mezzo della posta*".

### Caratteristiche salienti e giuridicamente rilevanti

#### Cosa è una PEC? Una busta!

Il processo di invio e ricezione della PEC può essere scomposto in vari passaggi e nella creazione di diversi oggetti. Insistendo sul paragone con una raccomandata A/R la PEC di per sé può essere rappresentata come una busta all'interno della quale sono contenute delle informazioni (la comunicazione, ovvero il testo della PEC e i documenti eventualmente allegati) trasportate dal mittente al destinatario.

Non a caso tra le definizioni contenute nel D.P.R. 68/2005 vi è quella di "*busta di trasporto*", proprio per indicare il tipo di operazione che si realizza con la PEC.

Si tratta quindi di uno strumento di trasporto e non di uno strumento di identificazione.

Il D.P.R. 68/2005 all'art. 1, lett. a), riporta - fra l'altro - la definizione di busta di trasporto che è "*il documento informatico che contiene il messaggio di posta elettronica certificata*". Lo stesso art. 1, lett. f), poi, definisce il messaggio di posta elettronica certificata come "*un documento informatico composto dal testo*

*del messaggio, dai dati di certificazione e dagli eventuali documenti informatici allegati".*

Se la PEC è la "busta di trasporto" e gli allegati eventuali al messaggio di posta elettronica sono documenti informatici, cosa è appunto il messaggio di posta elettronica (il "corpo" della comunicazione di posta elettronica)? E' null'altro che una seconda busta a cui sono allegati dei documenti.

Quindi la differenza principale con la Raccomandata A/R è che la PEC è composta in pratica da 2 "buste": una di trasporto vero e proprio e una che è il testo della mail al quale possono essere o meno allegati i documenti informatici.

In sostanza le fasi attraverso cui avviene spedizione e ricezione della PEC sono::

- 1.il messaggio di posta elettronica certificata viene inviato al server del gestore di PEC (un ente terzo certificato ed accreditato). Eventualmente il mittente avrà allegato alla PEC, a corredo del semplice messaggio di posta, i documenti informatici che possono o meno essere firmati digitalmente.
2. L'ente gestore verifica l'identità del mittente mediante la corrispondenza delle credenziali di accesso (login e password)
3. L'ente gestore predispone la ricevuta di accettazione che viene inviata al mittente (ovvero dice al mittente: "Tutto ok, la tua PEC è conforme e sta per essere girata al destinatario"); si tratta di una ricevuta che costituisce valore legale dell'avvenuta (o mancata) trasmissione del messaggio, con precisa indicazione temporale del momento in cui la mail PEC è stata inviata.
4. L'ente gestore "imbusta" il messaggio e gli eventuali allegati del mittente nella cosiddetta "busta di trasporto" e lo invia all'ente gestore della PEC del destinatario. Ovviamente i passaggi 3 e 4 avvengono in simultanea
5. L'ente gestore del destinatario verifica l'attendibilità della comunicazione e lo consegna nella sua casella.
6. L'ente gestore del destinatario produce a sua volta una ricevuta di avvenuta consegna al destinatario che viene inviata all'ente gestore del mittente che a sua volta la deposita nella casella del mittente.

Analogamente a quanto avviene con le raccomandate A/R chi invia un messaggio di posta elettronica certificata, ha quindi sia il modo di attestare la data dell'invio della comunicazione, che la possibilità di sapere se il suo messaggio è arrivato o meno a destinazione, tramite la ricevuta di ritorno.

Inoltre la PEC, essendo un metodo di trasmissione digitale, porta con sé diversi vantaggi. Non solo la trasmissione del messaggio di PEC e dei suoi allegati è immediata, sicura e garantita, ma il costo dell'invio di un messaggio di posta elettronica certificata, è gratuito (fermo restando il canone annuo da corrispondere al gestore per poter fruire di una casella PEC).

Una notazione finale relativa alla prova di consegna, ai sensi dell'art. 6 del D.P.R. 68/2005, le ricevute (di accettazione e di avvenuta consegna) inviate dal gestore di PEC costituiscono rispettivamente "*prova dell'avvenuta spedizione di un messaggio di posta elettronica certificata*" e "*che il suo messaggio di posta elettronica certificata è effettivamente pervenuto all'indirizzo elettronico dichiarato dal destinatario e certifica il momento della consegna tramite un testo, leggibile dal mittente, contenente i dati di certificazione.*" In questo senso l'art. 9 del D.M. 2.11.2005 dispone che "*a ciascuna trasmissione è apposto un unico riferimento temporale*", ossia viene attribuita la data certa.

### **Avvisi delle PEC, Ricevute, Buste**

Esistono quindi, a maggior tutela del mittente e del destinatario, ai sensi dell'art. 6, comma 6, del citato D.M. 2.11.2005 3 tipi di ricevuta ovvero: a) ricevuta di accettazione; b) ricevuta di presa in carico; e) ricevuta di avvenuta consegna completa. Si tratta dei 3 tipi di ricevuta che abbiamo affrontato nel segmentare il processo di invio e ricezione di un messaggio PEC.

Gli enti gestori non accettano messaggi con Virus Informatici o con sospetti virus informatici. In questi casi comunicano al mittente l'impossibilità di dare corso alla trasmissione e consegna del messaggio in quanto non lo possono verificare e lo conservano comunque per 30 mesi. In particolare gli avvisi, ai sensi dell'art. 6, comma 8, del citato D.M. sono: a) avviso di non accettazione per eccezioni formali ovvero per virus informatici; b) avviso di rilevazione di virus informatici;

e) avviso di mancata consegna per superamento dei tempi massimi previsti ovvero per rilevazione di virus informatici. Gli avvisi sono emessi in vari modi, in particolare tramite la Busta di anomalia: si tratta di un secondo tipo di busta che al contrario della “busta di trasporto” serve a segnalare appunto una anomalia. Si tratta quindi di un sistema impiegato dall’ente gestore PEC per “imbustare” i messaggi non a norma (ad esempio quelli spediti da un normale indirizzo di posta elettronica ad uno PEC), ovvero che hanno fatto riscontrare elementi di non conformità durante i controlli automatici effettuati dal server, nel momento di presa in carico del messaggio. Si tratta dunque di un avviso di non conformità che viene evidenziata dal fatto che il messaggio è inserito dentro la busta di anomalia.

A differenza della busta di trasporto, firmata dal gestore PEC mittente, la busta di anomalia è sottoscritta dall’ente gestore PEC destinatario e permette al mittente, preso atto dell’anomalia riscontrata dal sistema, comunque di accedere al messaggio e risolvere la non conformità riscontrata.

### Gli allegati della PEC

In base al principio della non modificabilità del messaggio PEC è garantita l’impossibilità di modificare sia il messaggio che gli allegati alla PEC; in base al fatto che il contenuto è criptato, non è assolutamente possibile attribuire la paternità di un documento informatico allegato al messaggio di PEC al mittente dello stesso messaggio.

La paternità di un documento può essere riconosciuta unicamente con l’apposizione della firma (elettronica o digitale), ma non è legalmente corretto assumere che il file allegato ad una email di PEC sia attribuita al mittente.

Il fatto che la busta di trasporto sia firmata elettronicamente può far cadere nell’errore: tuttavia ciò non è possibile in quanto la firma viene apposta da un soggetto terzo rispetto a mittente e destinatario (l’ente certificatore) che è il gestore di PEC. La firma apposta dall’ente certificatore garantisce la sola immutabilità del messaggio e non può attribuire la paternità degli allegati del messaggio medesimo al mittente.

## **Obbligo della PEC**

### **Obbligo per i cittadini**

Per il cittadino non sussiste, ad oggi, un obbligo normativo a dotarsi di una PEC ma molte amministrazioni richiedono l'uso della PEC per poter effettuare on line operazioni che finora erano effettuate solo "allo sportello". Tipico il caso del cambio di residenza online. Oltre tutto l'istituzione della Anagrafe Nazionale e l'entrata in vigore del regolamento europeo EIDAS (vedi più avanti nel capitolo dedicato) porteranno certamente ad ampliare i casi in cui senza un "domicilio digitale" (e quindi probabilmente una qualche sorta di PEC) sarà impossibile accedere ad alcuni servizi. Riguardo ai cittadini, diversamente da quanto accade per le imprese e per i professionisti, per i quali la PEC è obbligatoria e che per loro stessa natura possiedono competenze informatiche e commerciali adeguate, si pone il problema delle competenze necessarie per l'uso dei nuovi strumenti informatici.

Va notato in modo esplicito che proprio perché gli strumenti di cui parliamo sono fortemente legati alla natura informatica delle procedure e dei programmi ad essi sottostanti, i cambiamenti sono continui, sia per il diffondersi di tecniche e strumenti più performanti, sia per l'abitudine, purtroppo assai diffusa nel campo informatico a procedere per "aggiustamenti successivi". (E' nota la quantità, talvolta abnorme, di aggiornamenti per tutti i software, spesso rilasciati per riparare falle di sicurezza o veri e propri "bachi").

Poiché i software si appoggiano a sistemi operativi e browser che, per motivi tecnici o più spesso commerciali, vengono frequentemente modificati o aggiornati (senza garantire sempre una compatibilità "all'indietro") ne deriva la necessità di un continuo controllo del corretto funzionamento dei software sottostanti agli strumenti informatici qui trattati.

Va anche considerato che le caselle di PEC (come pure la firma elettronica e la marca temporale) devono essere acquisite da imprese e cittadini sul libero mercato, cosa non sempre agevole per chi non possiede le competenze necessarie a districarsi nelle innumerevoli offerte presenti sul mercato stesso.

E' pur vero che presso gli organi competenti vengono tenuti elenchi delle imprese abilitate a rilasciare PEC ed altro, ma spesso tali elenchi sono puramente indicativi e alcune delle istanze ivi riportate -come gli enti regionali- in realtà non hanno valenza pubblica dato che non è possibile per il comune cittadino accedere ai loro servizi e la loro presenza nell'elenco delle imprese abilitate appare quantomeno discutibile<sup>18</sup>. Probabilmente la soluzione sta nella possibilità di accedere ai servizi della PA con metodi più semplici e in questa direzione sembra andare l'introduzione dello SPID e alcune disposizioni sui siti Web della PA che prevedono modalità di interazione con cittadini e imprese che non fanno ricorso alla PEC.

### **Obbligo per professionisti e imprese**

I professionisti e le imprese, ai sensi dell'art. 16, comma 7, del Decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, nella Legge 28 gennaio 2009, n. 2, devono dotarsi di una casella di PEC e comunicarla al proprio Ordine professionale se professionisti o al Registro Imprese della propria provincia se imprese. Le ditte individuali hanno infine seguito anch'esse lo stesso destino: per loro l'obbligatorietà di una casella PEC è scattata con il Decreto Legge n. 179 del 2012 che inoltre stabilisce un indice nazionale degli indirizzi PEC delle imprese e dei professionisti tenuto dal Ministero dello Sviluppo Tecnologico di cui si parla più ampiamente più avanti.

### **Obbligo per la PA**

L'obbligo della PEC nella Pubblica Amministrazione, in particolare per le comunicazioni interne e tra le varie istanze della PA parte da lontano, ribadito nel CAD e confermato in diversi atti e disposizioni.<sup>19</sup>

Già il DPCM del 31 ottobre 2000 prevedeva, che gli indirizzi di posta associati al protocollo fossero comunicati al CNIPA che doveva gestirli attraverso l'Indice delle amministrazioni pubbliche. Ovviamente il CAD sancì già nella sua prima formulazione l'uso della Posta Elettronica Certificata “*per ogni scambio di*

---

<sup>18</sup> <http://www.agid.gov.it/node/2251>

<sup>19</sup> Qui il termine PA va inteso in senso ampio e comprende ad esempio anche gli enti non territoriali di vario tipo come le camere di commercio. Vedi a proposito:  
<http://www.lineaamica.gov.it/risposte>

*documenti e informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata”<sup>20</sup>.*

Inoltre lo stesso CAD ha stabilito che “*entro otto mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni centrali provvedono a istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata ... per ciascun registro di protocollo*”<sup>21</sup>

L’obbligo è stato ribadito dal decreto legge 29 novembre 2008, n. 185.

La legge 102 del 3 agosto 2009 ha istituito poi l’Indice degli indirizzi delle pubbliche amministrazioni. L’obbligo della posta elettronica e in particolare della PEC è dunque chiaramente sancito ma addirittura la [circolare n. 1/2010/DDI](#) (Dipartimento Digitalizzazione e Innovazione della Presidenza del Consiglio) ricorda che “*La mancata disponibilità di almeno una casella di Posta Elettronica Certificata per ciascun registro di protocollo e la prosecuzione delle tradizionali forme di comunicazione configurano l’inosservanza di disposizioni di legge e una fattispecie di improprio uso di denaro pubblico*”.

### **La conservazione dei messaggi e delle ricevute di PEC**

Secondo quanto previsto dall’art. 11, comma 2, D.P.R. 68/2005 il gestore di PEC ha l’obbligo di conservare i log (ovvero delle stringhe di testo da cui è possibile dedurre mittente, destinatario, esito della spedizione e data) dei messaggi per 30 mesi. Al termine di tale periodo il gestore non è più obbligato alla conservazione (ovviamente può continuare a farlo) dei log.

Sorge l’esigenza di avere sempre nella propria disponibilità il messaggio e le ricevute di PEC. È consigliabile quindi salvare i messaggi delle ricevute in modo da conservare memoria dell’avvenuto invio, ricezione, consegna eccetera. Tali documenti sono molto leggeri da un punto di vista informatico ma conservano informazioni fondamentali nel caso di controversia legale: in loro assenza non è possibile dimostrare l’invio, ricezione eccetera della PEC, analogamente a quanto avviene con la raccomandata A/R cartacea.

---

<sup>20</sup> Art 6 CAD

<sup>21</sup> Art 47 CAD

Le ricevute dei messaggi di PEC sono documenti informatici e poiché contengono la firma digitale del gestore non possono essere convertiti e/o trasformati in altri formati che siano diversi da quello originario (es. non si può salvare la ricevuta di in formato PDF) perché perderebbero le caratteristiche originarie. È possibile, quindi, salvare e conservare messaggi e ricevute di PEC sul proprio hard disk o su supporti esterni per poterne avere la disponibilità all'occorrenza ma al fine di evitare eventuali compromissioni dei dati salvati, potrebbe essere consigliato provvedere alla conservazione a norma di legge (CAD - D.Lgs. 82/2005 e DPCM 3/12/2013) così come indicato dall'articolo 44 del CAD. Il sistema di conservazione dei documenti informatici offre evidenti garanzie, poiché ai sensi dell'art. 43, comma 1, CAD "*i documenti così conservati sono validi e rilevanti a tutti gli effetti di legge*".

Nella remota ipotesi che fosse necessario il formato cartaceo, le ricevute dovranno essere stampate e munite della attestazione di conformità della copia analogica all'originale informatico secondo l'art. 9 della L. 53/1994 e le norme del CAD<sup>22</sup>.

Il problema della conservazione dei documenti, in particolare di quelli informatici, pone diverse questioni sia di tipo giuridico che tecnico. Di seguito un breve excursus per inquadrare quanto detto a proposito della conservazione dei messaggi PEC nel quadro più ampio del problema della conservazione documentale.

### **La conservazione dei dati “a norma di legge”**

Esistono delle regole tecniche per la conservazione a norma di legge dei documenti informatici. Queste regole tecniche sono tenute dall'AGID (Agenda per l'Italia Digitale già DIGITPA a sua volta CNIPA (Centro nazionale per l'informatica nella pubblica amministrazione) che ancora a sua volta sostituì nel 2003 l'AIPA (Autorità per l'informatica nella pubblica amministrazione (AIPA).

Le norme di riferimento sono contenute nel **DPCM del 3 dicembre 2013 (Regole tecniche in materia di sistema di conservazione)** che dava 3 anni di tempo (quindi fino alla fine del 2015) alle amministrazioni della PA per adeguarsi dal punto di

---

<sup>22</sup> Si tratta di apporre quello che viene definito contrassegno elettronico

vista tecnologico e di conseguenza anche organizzativo. Senza voler entrare nel merito specifico delle modalità di conservazione si precisa quanto segue.

Le regole tecniche si concentrano sulle modalità di protocollazione e conservazione dei documenti informatici ed originano dall'art. 40 del CAD che recita: “*Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice [...]*”

In sostanza la norma richiamata stabilisce un preciso obbligo: i documenti delle pubbliche amministrazioni devono essere prodotti esclusivamente in modalità informatica. Ecco dunque che al pari dei documenti cartacei anche i documenti informatici sono destinati ad essere conservati nel tempo ma, mentre per i documenti analogici le regole di archiviazione sono relativamente semplici, per i documenti informatici sono richiesti “particolari accorgimenti” in grado di garantire, durante l’intero ciclo di gestione degli stessi, il mantenimento del loro valore giuridico e legale.

L’art.44 del CAD determina i requisiti per la conservazione dei documenti informatici che sono richiamati e riassunti dall’ art. 3 comma 1 DPCM 3 dicembre 2013, nel quale si specifica che le regole tecniche garantiscono “*le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità*” dei documenti informatici.

Sempre il DPCM 3 dicembre 2013 istituisce la figura del responsabile della conservazione (art. 7) e il Manuale di gestione documentale (art.8); nell’art. 9 infine concentra la descrizione delle fasi di conservazione.

Lo scopo dunque è chiaro: rendere definitivamente e facilmente utilizzabili i documenti informatici procedendo lungo il percorso della quanto più completa possibile dematerializzazione delle PA, utilizzando strumenti informatici definiti a loro volta in altra normativa specifica (si pensi ad esempio al ruolo chiave della Firma digitale).

Il sito della AGID riporta a questo link le disposizioni operative per realizzare correttamente la conservazione (<http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione>)

## Vari tipi di PEC

La PEC è semplicemente la PEC. Questa affermazione lapalissiana non trova invece riscontro nella legislazione italiana. Infatti nel tempo si sono introdotti diversi tipi di PEC che hanno complicato la situazione normativa e introdotto dubbi interpretativi.

Infatti oltre alla PEC “semplice”, è esistita la CEC-PEC, è ancora attualmente presente nell’ordinamento la PEC ID, lo Schema di decreto di modifica del CAD sembra introdurre una PEC “virtuale”, un decreto del Consiglio di Stato pare introdurre una PEC con caratteristiche aggiuntive rispetto a quella ordinaria, nelle disposizioni che regolano le vendite telematiche viene introdotto un tipo ancora diverso di PEC. Insomma pare ci sia un po’ di confusione che non aiuta a districarsi nelle norme e soprattutto introduce specifiche che complicano la vita agli operatori. Infatti anche se non si tratta di PEC concettualmente diverse tra loro potrebbe rendere necessario, ad esempio per un avvocato che si occupi di questioni diverse, dotarsi di PEC diverse con buona pace della semplicità che gli strumenti elettronici dovrebbero introdurre. Riportiamo brevemente le caratteristiche dei vari tipi di PEC al fine di corroborare una delle tesi di questo lavoro: “troppe norme e troppo analitiche”.

### **PEC Semplice**

Si tratta della PEC “standard” che presenta tutte le caratteristiche classiche della PEC. Ha come abbiamo già visto lo scopo certificare le comunicazioni “ufficiali” nelle quali il mittente necessita della prova dell’invio e del ricevimento (o meno) del messaggio da parte del destinatario.

### **CEC-PAC**

Si tratta di un tipo specifico di PEC ora in disuso voluta nel 2010 dal Ministro Brunetta e che negli intenti del ministro sarebbe dovuta servire per tutte le comunicazioni tra cittadini e PA. Nasce in seguito al DPCM del 6 maggio 2009 che stabiliva che il "Dipartimento per la digitalizzazione della Pubblica Amministrazione e per l’innovazione tecnologica"assegnasse a titolo non oneroso, a ogni Cittadino che ne facesse richiesta, un indirizzo di Posta Elettronica Certificata da utilizzare per tutte le comunicazioni con la Pubblica

Amministrazione. Il sito di riferimento è <https://www.postacertificata.gov.it/> e fino al momento della sua progressiva dismissione al sito si erano registrate 2.121.915 persone. Il sistema è in corso progressivo di disattivazione (l'accesso agli utenti registrati sarà garantito fino al 2018, sebbene non sia già più possibile utilizzare la CEC-PAC) per fare convergere tutte le comunicazioni sui sistemi PEC standard. Questo sistema di PEC ha generato giudizi non solo discordanti ma addirittura opposti tra chi lo vedeva come una delle migliori riforme recenti<sup>23</sup>, e chi ne evidenziava limiti e difetti intrinseci<sup>24</sup>

All'indirizzo seguente le tappe della sospensione del servizio:  
<https://www.postacertificata.gov.it/home/sospensione-servizio.dot>.

### **PEC ID**

Si tratta di un particolare tipo di PEC cui è dedicato un intero Decreto (DPCM del 27 settembre 2012) che ne specifica in dettaglio le caratteristiche. La caratteristica saliente è che questo tipo di PEC integra in sé la firma digitale e quindi a norma si possono inviare con essa documenti che hanno la validità di documenti firmati digitalmente. Rimane aperta la questione degli allegati alla PEC che secondo alcuni, non essendo incorporati nel messaggio di PEC ma appunto semplicemente allegati, sarebbero da considerare documenti indipendenti e quindi da firmare comunque; la questione rimane aperta nel senso che, come esemplificato nel capitolo sulle sentenze non esiste una giurisprudenza unanime sulla questione. Dal punto di vista tecnico la differenza fondamentale sta nel modo di riconoscimento dell'assegnatario della casella di PEC, infatti trattandosi di un riconoscimento "forte" ovvero ottenuto previa identificazione del sottoscrittore, questo permette di attribuire alla PEC ID non solo funzione di trasmissione ma anche funzione di identificazione.

### **La PEC della Corte dei Conti**

Come verrà meglio analizzato nel paragrafo riguardante le Regole tecniche con un apposito decreto emanato il 21 ottobre 2015 la Corte dei Conti stabilisce l'uso esclusivo della PEC nei procedimenti davanti alla Corte medesima. Il fatto è che

---

<sup>23</sup> <http://www.ilfattoquotidiano.it/2014/12/18/cec-pac-addio>

<sup>24</sup> <http://sportelloconsumatori.org/blog/2014/12/20/muore-la-posta-certificata-statale>

le caselle di PEC usate (e quindi si presume anche quelle dei professionisti e delle varie istanze della PA coinvolte nei procedimenti dovranno, come già visto nel capitolo sulle Regole tecniche di requisiti aggiuntivi (*sistemi di protezione dall'invio di messaggi indesiderati* e particolari *requisiti dimensionali e tecnici minimi*) rispetto alle normali caselle di PEC. Quindi a rigor di logica qualcuno dovrà asseverare che le caselle PEC rispondono a questi requisiti per cui le "normali" caselle che non hanno questa asseverazione non dovrebbero essere valide, il che significa che la Corte dei Conti, sicuramente andando oltre le intenzioni, introduce un nuovo tipo di PEC che peraltro, stando alla lettera delle disposizioni risulterebbe piuttosto difficile da realizzare; infatti se tutte le caselle di PEC, per ovvi motivi hanno protezioni contro le minacce informatiche, realizzare un metodo "*di protezione dall'invio di messaggi indesiderati*" sembra più che complesso, impossibile.

### **La PEC delle aste telematiche**

Anche in questo caso le conseguenze di una norma paiono andare oltre le intenzioni e prefigurare un nuovo tipo di PEC che sembra ridondante rispetto alle necessità. Il decreto ministeriale 32 del 26 febbraio 2015 detta norme per le aste telematiche. Al di là di una analisi del decreto che esula da questo lavoro, qui basta notare che le caselle PEC tramite cui vanno inviate le offerte in caso di vendita immobiliare dovranno essere "*apposite caselle di posta elettronica certificata per la vendita telematica*", *rilasciate dal gestore a chi intende formulare un'offerta ed indirizzate ad un indirizzo pec del Ministero della giustizia*". La dizione "apposite" qui si riferisce al fatto che " *la posta elettronica certificata per la vendita telematica*", *definita alla lett. n) dell'art. 2 del Decreto, dovrà contenere l'attestazione del gestore della casella di posta elettronica certificata per la vendita telematica di aver provveduto al rilascio delle credenziali, previa identificazione del richiedente, a norma dello stesso Decreto n. 32/2015, come previsto espressamente dal comma 2 dell'art. 13.*" Non è chiaro perché si sia introdotta questa specifica anche perché probabilmente bastava un semplice richiamo alla PEC-ID (che peraltro non viene mai nominata e che pare del tutto dimenticata dagli stessi legislatori che l'hanno introdotta) e anche perché "*in alternativa l'offerta potrà essere trasmessa anche mediante casella di posta*

*certificata priva dei requisiti di cui sopra, laddove l'offerta sia firmata digitalmente*". Ancora una volta la tendenza a specificare in modo troppo dettagliato gli strumenti elettronici di cui si richiede l'uso sembra aver introdotto complicazioni non necessarie.

## Elenchi PEC

Essendo la PEC caratterizzata da un indirizzo e-mail è auspicabile la maggiore pubblicità possibile e la più facile accessibilità a questi indirizzi. A questo scopo sono stati creati diversi elenchi pubblici e agevolmente consultabili di indirizzi PEC, alcuni dei quali stabiliti da apposite norme di legge. Di seguito un elenco dei più importanti.

### INI PEC

L'INI-PEC è l'Indice Nazionale degli Indirizzi di Posta Elettronica Certificata istituito dal Ministero dello Sviluppo Economico. Ha un proprio sito (<https://www.inipec.gov.it/>) e serve a raccogliere le PEC di professionisti ed imprese in Italia.

Come già visto, il CAD è considerato come il primo grande passo per rendere più efficienti e innovativi i rapporti tra cittadini e istituzioni, ed è costituito da un insieme di norme che favoriscono e regolamentano le comunicazioni digitali tra la Pubblica Amministrazione e i cittadini. Tra le altre innovazioni, il CAD con l'articolo 6, introduce la possibilità da parte della Pubblica Amministrazione di utilizzare la PEC per ogni scambio di documenti e informazioni con i soggetti che ne hanno fatto preventivamente richiesta. Con la legge 28 gennaio 2009, n.2 (conversione del decreto legge 29 novembre 2008, n.185) viene introdotto l'obbligo (art. 16) da parte delle imprese e dei professionisti di avere un indirizzo di PEC proprio e di comunicarlo rispettivamente al Registro Imprese e agli Ordini o Collegi di appartenenza.

Con il decreto legge 18 ottobre 2012, n.179 (convertito con modificazioni dalla legge 17 dicembre 2012, n.221), all'articolo 5, commi 1 e 2, questo obbligo viene esteso anche alle imprese individuali, siano esse nuove o già esistenti.

In sostanza al 30 giugno 2013 è stato compiuto progressivamente il processo per il quale tutti i professionisti, le aziende e le imprese individuali hanno l'obbligo di dotarsi di un proprio indirizzo PEC.

All'interno dell'articolo 5, al comma 3 del decreto legge 18 ottobre 2012, n.179, viene apportata una modifica del CAD: dopo l'articolo 6 viene infatti introdotto l'articolo 6bis che sancisce la nascita dell'INI-PEC a partire dagli elenchi di indirizzi PEC già registrati presso il Registro delle Imprese e gli Ordini o Collegi professionali di appartenenza dei singoli professionisti, come già previsto dall'articolo 16 del decreto legge 29 novembre 2008, n.185.

Tutte le operazioni per la creazione dell'INI-PEC sono sovrintese dal Ministero dello Sviluppo Economico che, sentita l'Agenzia per l'Italia digitale, con il decreto attuativo del 19 marzo 2013, emana le norme che regolamento tempi e modalità sia della raccolta che dell'aggiornamento degli indirizzi di posta elettronica certificata messi a disposizione nel portale INI-PEC.

Ad oggi (fine marzo 2016) sono disponibili oltre 1.250.000 indirizzi PEC di professionisti relativi a circa 1.700 ordini e collegi professionali, e oltre 4.625.000 indirizzi PEC di imprese (società e imprese individuali). Ovviamente l'indice è in continuo aggiornamento.

## **REGINDE**

Il Registro Generale degli Indirizzi Elettronici (ReGIndE), gestito dal Ministero della Giustizia, contiene i dati identificativi nonché l'indirizzo di posta elettronica certificata (PEC) dei soggetti abilitati esterni, ovverossia di quanti intervengono nei procedimenti giudiziari senza essere appartenere ai ruoli del Ministero stesso cioè: i) appartenenti ad un ente pubblico, ii) professionisti iscritti in albi ed elenchi istituiti con legge; iii) ausiliari del giudice non appartenenti ad un ordine di categoria o che appartengono ad ente/ordine professionale che non abbia ancora inviato l'albo al Ministero della giustizia (questo non si applica agli avvocati, il cui specifico ruolo di difensore implica che l'invio dell'albo deve essere sempre fatto dall'ordine di appartenenza o dall'ente che si difende). La registrazione al ReGIndE avviene con modalità diverse a seconda dei soggetti interessati: si va dalla trasmissione obbligatoria per alcuni ordini alla richiesta di registrazione

autonoma e personale, alla richiesta effettuata tramite un punto di accesso, per cui ReGlndE viene popolato dalle comunicazioni periodiche al Ministero da parte dell'Ordine professionale e da parte delle camere di commercio per quanto riguarda le imprese oltreché dagli indirizzi PEC delle amministrazioni pubbliche. Si tratta di un registro di grande rilevanza e la cui buona tenuta è essenziale poiché gli indirizzi qui contenuti sono coinvolti in tutte le fasi del processo telematico nelle sue diverse articolazioni.

## IPA

L'Indice delle Pubbliche Amministrazioni (IPA) è l'archivio ufficiale degli Enti pubblici e dei Gestori di pubblici servizi. L'Agenzia per l'Italia digitale si occupa di realizzare e gestire questo indice che contiene molte informazioni sui diversi Enti e sulla loro struttura.

Per quello che ci riguarda contiene anche gli indirizzi di posta certificata di tutti gli enti pubblici e dei gestori di pubblici servizi, può essere consultato liberamente via web ed è aggiornato periodicamente a cura degli stessi Enti.

All'IPA si accede tramite il sito:

<http://www.indicepa.gov.it/documentale/index.php>

## PEC degli Uffici Giudiziari

Le informazioni sui servizi telematici attivi presso gli Uffici Giudiziari e tutti gli indirizzi di posta elettronica associati agli uffici giudiziari sono reperibili all'indirizzo [http://pst.giustizia.it/PST/it/pst\\_2\\_4.wp](http://pst.giustizia.it/PST/it/pst_2_4.wp).

Si tratta di un registro che ha ovviamente particolare importanza nell'ambito processuale a tutti i livelli, ma gli indirizzi PEC ivi riportati sono esclusivamente adibiti a funzioni processuali. Lo stesso sito precisa infatti: “*Si evidenzia che gli indirizzi di Posta Elettronica Certificata associati agli uffici giudiziari devono essere utilizzati esclusivamente per il deposito telematico di atti e documenti processuali da parte di soggetti abilitati, come indicato nell'art 4 del D.M. 44/2011. Messaggi di natura diversa verranno automaticamente scartati*”

## PUNTI CRITICI della PEC

Vale anche la pena di accennare al fatto che la complessa normativa italiana sulla PEC e la firma digitale viene messa in discussione da più parti, non solo per la accennata complessità ma anche per incompatibilità con alcuni software commerciali molto diffusi.

Ad esempio riportiamo un parere dell'ISCOM (Istituto Superiore delle Comunicazioni ente di tipo tecnico-scientifico, considerato la massima autorità del settore con ruolo di consulenza del Ministero dello Sviluppo Economico nell'ambito dell'effettiva applicazione della normativa, della formazione e della istruzione specializzata in tutte quelle materie che sono connesse in particolar modo con lo sviluppo tecnologico) che a seguito di richieste da parte di alcune associazioni dichiara: “*La PEC non è dunque interoperabile e, proprio perché non basata su uno standard internazionale, non è integrata in alcuni software commerciali di gestione della posta come, ad esempio, Microsoft Exchange Server.*”<sup>25</sup> citare fonte.

Si tratta quindi di una critica di fondo: ovvero al fatto che la PEC è un sistema piuttosto “autarchico”, nel senso che risulta in uso praticamente solo in Italia, mentre a livello europeo già da qualche anno sono stati definiti degli standard di comunicazione che possono essere implementati usando gli abituali software di gestione della posta elettronica ordinaria e non necessitano, per il loro funzionamento, della costruzione di complessi sistemi centralizzati di gestione. Sempre l'ISCOM afferma: “*La IETF (Internet Engineering Task Force) ha elaborato un “Internet standards track protocol” (RFC 3798) per la posta elettronica, che, analogamente, garantisce le funzionalità 1) e 2) (conferma ricezione email) e, a differenza della PEC non implica la creazione di un sistema centralizzato per la gestione degli aspetti di sicurezza. Di fatto lo standard può essere implementato utilizzando i software commerciali di gestione della posta.*”

I problemi che potrebbero nascere dalla scarsa interoperabilità con standard internazionali saranno oggetto di un capitolo successivo dove si analizzano gli scenari legati all'entrata in vigore del regolamento eIDAS.

---

<sup>25</sup><http://www.cittadininternet.it/2013/04/07/pec-incompatibile-lo-dice-iscom>

L'importanza del parere dell'ISCOM in Italia in un settore in cui è considerato il massimo ente, è pari al valore che generalmente si tende ad attribuire nell'ambito della cosiddetta “soft law” ad organismi internazionali nell'ambito economico e finanziario. Si tratta dunque di orientamenti e riflessioni che, al di là dello stretto valore legale, assumono una importanza fondamentale nella determinazione delle prassi da parte delle imprese, della PA e dei singoli cittadini e non da ultimo nel fare assumere a Governo e Parlamento eventuali correzioni a pratiche considerate errate e/o obsolete nel campo di interesse.

Le critiche al sistema di PEC provengono da più parti e riguardano diversi punti della normativa e della attuazione pratica di questo strumento. Si tratta quasi sempre di osservazioni non prive di senso ma va ribadito che probabilmente proprio la volontà di introdurre tempestivamente i nuovi strumenti elettronici di trasmissione e firma certificata hanno indotto a creare un sistema che risente del precoce utilizzo di PEC e FE e che sembra stentare a stare al passo con l'innovazione tecnologica. Riportiamo a titolo di esempio, senza entrare nel dettaglio delle argomentazioni in essi presenti, alcuni articoli sugli aspetti più critici della PEC.

Nell'articolo reperibile in <https://archiviando.wordpress.com/2015/02/23/la-pec-un-prodotto-made-in-italy/> si critica la PEC in quanto troppo complessa e gli si contrappone il sistema S/MIME più semplice soprattutto, secondo l'estensore dell'articolo, dal punto di vista della conservazione, peraltro richiesta obbligatoriamente dalle legge, dei vari “pezzi” che compongono la PEC (Avvisi, buste, ricevute).

Nell'articolo reperibile in <http://www.wired.it/economia/lavoro/2014/03/03/posta-elettronica-certifica-abolire-petizione-change-org/> si pone l'accento sul fatto che la PEC, a differenza di altri sistemi certificati dalla IEFT (International Engineering Task Force, l'unica autorità internazionale demandata agli standard su Internet) non è interoperabile con gli analoghi sistemi di altri paesi europei, critica questa in realtà evidenziata da più parti ma che dovrebbe essere superata con l'adeguamento della normativa italiana a eIDAS.

Infine nell'articolo reperibile in <http://www.dirittodisapere.it/2015/09/03/pec-comunicare-con-la-pubblica-amministrazione-costa/> si mette l'accento sul fatto che l'esercizio di un diritto che la legge per prima definisce prioritario, ovvero la possibilità di comunicazione con la PA sia, dopo il fallimento del progetto Posta Certificat@<sup>26</sup>, a pagamento.

---

<sup>26</sup> a ogni cittadino che ne avesse fatto richiesta veniva fornita gratuitamente una casella di posta elettronica certificata chiamata CEC PAC con estensione “@postacertificata.gov.it

## LA FIRMA ELETTRONICA

Si fa riferimento in questo paragrafo soprattutto al **decreto del presidente del consiglio dei ministri del 22 febbraio 2013** (G.U. n. 117 del 21 maggio 2013) che è la normativa più recente in materia ed è rubricato *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali.*

Va detto, anche in questa occasione, che abbiamo a che fare con un decreto che, dando attuazione al CAD del 2005, lo modifica in parte in conseguenza di normative successive al CAD stesso (in questo caso in particolare il decreto legislativo n. 235/2010).

Ad esempio, con l'aggiunta della nuova lettera q-bis dell'art 1, comma 1 del D.lgs. 82/2005 (fatta appunto tramite il DL 235/2010) è stato reintrodotto, in Italia, il concetto di **firma elettronica avanzata**.

Tale firma, già presente in Italia in seguito al recepimento della direttiva comunitaria 1999/93/CE, era stata eliminata nel 2005 con l'introduzione del “primo” CAD che non ne faceva più menzione, contenendo solo i concetti di firma elettronica, firma elettronica qualificata e firma digitale, ma è stata reintrodotta per dare “*un quadro completo di firme elettroniche che tiene conto delle differenti soluzioni tecnologiche utilizzabili ai fini di garantire la corretta associazione di un documento ad un soggetto e l'integrità del documento stesso*”. A prescindere dagli scopi alla base di tale reintroduzione, va notato come sia piuttosto facile incappare in un groviglio di norme e definizioni conseguenti non sempre facile da districare soprattutto a posteriori.

Molto probabilmente con la reintroduzione della firma elettronica avanzata si è voluto dare un concreto valore giuridico a strumenti di firma che non prevedono l'uso di certificati qualificati ma che, comunque, garantiscano l'univoca interconnessione con il firmatario, ne permettano la corretta identificazione e consentano l'individuazione di eventuali modifiche ai dati firmati. Tali strumenti, in effetti, potrebbero risultare utili in tantissimi casi in cui, più che di vera e propria firma/sottoscrizione, sia necessario ricorrere ad una firma/visto che

assolva esigenze di sicurezza e integrità del documento piuttosto che di paternità e/o appropriazione del contenuto.

Oltre a quanto definito nell'ambito della normativa nazionale, in questo lavoro si è dovuto tenere anche presente della nuova definizione (o meglio: della nuova “meta-definizione”, nel senso di una definizione che contiene quelle di tutte le firme, che potremmo intendere come *genus* rispetto alle diverse tipologie di firma che possiamo considerare come *species*)<sup>27</sup> del Regolamento eIDAS di cui si parlerà dettagliatamente in un prossimo capitolo. Qui basta mettere in evidenza che eIDAS parla di soli 3 tipi di firme elettroniche, mentre la normativa italiana di 4 tipi; inoltre dalla definizione poco sopra data in nota si evince come eIDAS mette l'accento sulla funzione dichiarativa della firma, mentre il CAD la pone sulla funzione identificativa.

La diversa funzione che la firma assume nei vari contesti è stata oggetto di analisi dal punto di vista giuridico ben prima dell'introduzione della firma elettronica e il testo di riferimento per questa questione viene considerato addirittura il Cornelutti<sup>28</sup> del 1939. Va sottolineato che la questione del ruolo e del significato della firma assume importanza particolare proprio con l'introduzione degli strumenti elettronici. Infatti nell'interpretazione di questi strumenti, per la loro stessa natura e per la novità sostanziale che rappresentano rispetto agli strumenti analogici, non è possibile rifarsi né al senso comune né agli usi consolidati.

Di qui l'obbligo di definire con chiarezza e sufficiente analiticità i termini e i concetti coinvolti nelle normative sugli strumenti elettronici di cui trattiamo, cosa che porta a elenchi lunghissimi di definizioni (in eIDAS all'art. 3 sono riportate 43 definizioni, nel CAD all'art.1 (Definizioni) si esauriscono tutte le lettere dell'alfabeto nonostante u bis, ter e quater).

D'altra parte gli strumenti informatici sono sostanzialmente algoritmi definiti *passo passo* nelle loro caratteristiche anche di dettaglio minuto, il che comporta la necessità di approfondire l'analisi dei diversi significati che la firma assume. Anche senza voler approfondire troppo la questione appare abbastanza evidente

---

<sup>27</sup> eIDAS definisce la firma elettronica come “*dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.*”

<sup>28</sup> Cornelutti: *Studi sulla sottoscrizione* in *Studi di Diritto Processuale*, III, Padova, 1939

che potrebbero essere necessari strumenti diversi per svolgere, dal punto di vista informatico, le diverse funzioni di una sottoscrizione che vanno dalla attestazione di provenienza del documento alla accettazione, all'identificazione, la presa visione, l'autenticazione, l'attestazione di conformità e così via

Ma cos'è la firma elettronica in senso lato? E', sul piano informatico, l'equivalente della firma olografa da utilizzare però per i documenti informatici: se per imputare un documento cartaceo ad un soggetto, nella maggior parte dei casi, si ricorre alla apposizione di una firma olografa, per il documento informatico si è reso necessario concepire una **sottoscrizione elettronica** (non utilizziamo immediatamente il termine firma per non ingenerare confusione a causa dei diversi tipi di firma esistenti) in grado di garantire il legame tra firmatario e documento informatico sottoscritto.

La sottoscrizione elettronica non è semplicemente un atto (come l'apposizione della firma olografa) ma si tratta bensì di un processo informatico basato su algoritmi crittografici che permettono di legare un documento informatico ad un insieme di dati in forma elettronica (la cosiddetta "firma") propri di uno specifico soggetto; tale processo è ufficialmente e legalmente riconosciuto come metodo univoco di identificazione informatica di un soggetto e serve per attribuire senza dubbio (a meno di querela di falso) un dato documento informatico ad un dato soggetto.

Quel che per il momento sembra certo è che, al pari della firma digitale e delle altre firme elettroniche qualificate, la firma elettronica avanzata permetterà ai documenti firmati di avere lo stesso valore probatorio riconosciuto alle scrittura private.

Considerazioni di questo tipo, che possono essere fatte non solo per la firma elettronica ma per tutti gli altri argomenti trattati da eIDAS e CAD, inducono molti esperti a ritenere che sia giunto il momento di una sorta di testo unico che metta ordine nella materia. Oltre tutto le stesse definizioni date nel DPCM del 22 febbraio 2013 sono molto tecniche e mentre per firma elettronica e digitale fanno riferimento a quanto contenuto nel CAD, introducono alcune nuove nozioni piuttosto complesse; ad esempio si parla di: i) **firma remota**: 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; ii) **firma automatica**: 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. Si tratta di strumenti nati per agevolare quanti devono “firmare per legge” grandi quantità di documenti (si pensi alla certificazione rilasciata dagli uffici anagrafici o alle comunicazioni dell’Agenzia delle Entrate) e non possono, per motivi di tempo o di fattibilità pratica, farlo “di persona”. Il problema è, al solito, nell’uso di norme di rango inferiore rispetto al CAD, per introdurre concetti nuovi e dal CAD non esplicitamente previsti.

### Il documento informatico ed il documento amministrativo

La firma elettronica viene apposta su un documento elettronico e quindi, prima di passare alle definizioni di firma sembra opportuno richiamare in breve l’attenzione sul concetto di documento informatico, ovvero del documento elettronico ormai completamente equiparato, se trattato nelle opportune modalità, al documento cartaceo. Il documento informatico trova la sua definizione principale nel CAD ed è il frutto delle evoluzioni che hanno riguardato questo ambito, e ne va sottolineata l’importanza come elemento indispensabile per la informatizzazione dell’azione amministrativa. Il documento informatico<sup>29</sup> è definito all’art.1 comma p) come “*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*”, mentre con il comma p-bis si definisce il documento analogico come “*la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*”. Qui addirittura il concetto più “vecchio”, quello di documento analogico viene definito “*in negazione*” rispetto al più nuovo<sup>30</sup>.

---

<sup>29</sup> Non entriamo qui nella questione che però va segnalata come non irrilevante della confusione che spesso si ritrova quando in modo intercambiabile si parla di documento elettronico, informatico o digitale o addirittura telematico.

<sup>30</sup> eIDAS introduce una nuova definizione, peraltro inserita nel CAD dall’emanando decreto di modifica più volte citato, che appare, una volta tanto meno pregnante ed efficace della definizione data dalla legislazione italiana; infatti in eIDAS il documento informatico viene definito come “*qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva*”

Per arrivare ad una completa e chiara definizione di documento amministrativo informatico, è necessario richiamare quanto disposto dalla normativa riguardo al documento amministrativo. In particolare va ricordato che l'art. 22, comma 1, lett. d), della Legge 7 agosto 1990, n. 241, afferma che per documento amministrativo, si intende “*ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale*”.

Una definizione che guarda al documento amministrativo da una angolazione leggermente diversa è quella del Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (D.P.R. 28 dicembre 2000, n. 445 (G.U. n. 42 del 20 febbraio 2001) e modificazioni successive), che all'art. 1, comma 1, lett. a), definisce il documento amministrativo come “*ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa*”.

In realtà il concetto di documento informatico, anche se nelle grandi linee è ben definito, è un concetto in evoluzione<sup>31</sup> come messo in evidenza da molti autori e, nonostante il largo accordo sul suo pieno valore giuridico, ribadito da diverse norme, alcune sue caratteristiche come la necessità di strumenti appositi per leggerlo, il fatto che sia scritto su supporti facilmente deperibili, la necessità della sua conservazione con modalità particolari ed altre sue fondamentali caratteristiche rendono necessario analizzare approfonditamente il concetto di documento digitale e tutte le sue implicazioni giuridiche o sociali<sup>32</sup>.

Risulta anche rilevante il problema della trasformazione di un documento analogico in informatico e viceversa.

---

<sup>31</sup> Il “documento digitale”: analisi di un concetto in evoluzione in DigItalia Web vol.1 (2008) reperibile all’indirizzo <http://digitalia.sbn.it/article/view/440>

<sup>32</sup> Basterà qui ricordare la complessità delle questioni legate alla privacy emerse nel recente braccio di ferro tra l’Amministrazione Statunitense e la Apple sull’utilizzo dei file contenuti negli smartphone di sospetti terroristi ai fini processuali e di indagine.

Infatti anche se lo scopo della introduzione degli strumenti informatici nei procedimenti amministrativi è il passaggio integrale al digitale e la progressiva eliminazione del cartaceo ci sono almeno due casi in cui la conversione da un documento di tipo informatico ad uno analogico o viceversa si rende ancora indispensabile.

Il primo caso, più ovvio, è quello della digitalizzazione degli archivi cartacei di vario tipo ai fini anche di eliminare fisicamente i documenti su supporto cartaceo quando questi non rivestano particolare valore storico o archivistico e procedere alla sola archiviazione cartacea con risparmio in termini di spazi e facilità di consultazione dei nuovi archivi così formati. Si tratta come è evidente di una questione della massima importanza economica ma che riveste grande rilevanza anche dal punto di vista storico, archivistico e scientifico<sup>33</sup> ed ovviamente giuridico come nel caso della digitalizzazione degli atti notarili di varia natura.

In questo caso la legge detta norme perché il passaggio analogico-digitale avvenga con tutte le garanzie di conformità all'originale e di inalterabilità del documento elettronico generato. In questo processo gioca un ruolo importante la firma elettronica e in particolare quella digitale. Infatti il CAD nel comma 6 dell'art. 22 riferendosi alle copie digitali di documenti analogici dispone che “...*in casi di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico*”.

Anche il passaggio inverso cioè dal digitale all'analogico viene normato nel dettaglio. Si tratta di un caso che appare assai meno ovvio di quello precedente. Infatti se la conversione da analogico a digitale ha gli scopi e i vantaggi appena descritti, che senso ha far diventare analogico un documento che nasce digitale? La cosa è meno strana di quello che sembra. Infatti questo passaggio è previsto esplicitamente dal CAD nell'articolo 3-bis (domicilio digitale del cittadino), commi 4-bis, 4-ter e 4-quater, nel caso in cui il cittadino non abbia domicilio

---

<sup>33</sup> Basta pensare alla quantità immensa di documenti storici posseduti soprattutto dai paesi di più antica tradizione archivistica e all'importanza della loro disponibilità per gli studiosi di varie discipline non solo storiche.

digitale, poiché in questo caso le amministrazioni possono predisporre le comunicazioni al cittadino come documenti amministrativi informatici sottoscritti con firma digitale o firma elettronica avanzata, da conservare nei propri archivi, ed inviano al cittadino, per posta ordinaria o raccomandata con avviso di ricevimento, le copie analogiche di tali documenti amministrativi informatici sottoscritte con firma autografa sostituita a mezzo stampa. In questa specifica situazione viene introdotto un nuovo strumento che con un po' di fantasia potremmo chiamare l'equivalente analogico della firma digitale. Si tratta di quello che viene chiamato sulla base dell'art. 23ter del CAD (documenti amministrativi informatici), contrassegno elettronico<sup>34</sup>. Al comma 5 del citato art.23 il CAD recita infatti: " *Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno....Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa...*" Si tratta di uno strumento che ha suscitato alcune perplessità tra gli operatori<sup>35</sup> ma che appare necessario almeno fino a quando non sarà completato il passaggio integrale al digitale<sup>36</sup>.

### **Le definizioni di “firma”:**

Il CAD all'art. 1, comma 1, lettere q), q-bis), r), s), individua e disciplina quattro diverse tipologie di sottoscrizione elettronica:

1. **firma elettronica** equivale a una firma personale associata a un documento scritto, per fornire una prova della sua provenienza. Il CAD la definisce come "*l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*";
2. **firma elettronica avanzata** garantisce la connessione univoca tra firmatario e documento. Sembra dunque trattarsi più di un processo che si

---

<sup>34</sup> Il contrassegno elettronico è noto anche come Timbro digitale, Codice bidimensionale o Glifo.

<sup>35</sup> Vedi per tutti: [http://www.anorc.it/notizia/253\\_Il\\_glifo\\_protegge\\_solo\\_se\\_stesso.html](http://www.anorc.it/notizia/253_Il_glifo_protegge_solo_se_stesso.html)

<sup>36</sup> Questa questione racchiude in sé un problema di natura “filosofica” che riguarda il documento elettronico. In quanto tale esso infatti risulta inconoscibile all’utente che non usi le adeguate tecnologie (un hard disk non può essere letto se non tramite un apparato elettronico complesso). L’unico documento che ad oggi l’essere umano è in grado di conoscere senza necessità di strumenti complessi è quello cartaceo (a condizione ovviamente che l’essere umano in questione sappia leggere e conosca la lingua in cui il documento è scritto)

sostanza in una serie di requisiti e di passaggi successivi di carattere documentale, identificativo e informativo piuttosto che di uno specifico tipo di firma. Il CAD la definisce un “*insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati*”;

3. **Firma elettronica qualificata:** è una firma avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma ovvero di mezzi sui quali il firmatario può conservare un controllo esclusivo. Il CAD la definisce “*un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma*”;
4. **firma digitale** è una firma elettronica che utilizza un sistema di due chiavi crittografiche, una pubblica e una privata, le cui caratteristiche, modalità di generazione/conservazione e requisiti di sicurezza vengono stabiliti nel Dpcm 22 febbraio 2013. Il CAD la definisce come “*un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario 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*”.

Sul piano probatorio i documenti firmati con la firma elettronica e la firma elettronica avanzata sono liberamente valutabili sulla base delle caratteristiche di qualità e sicurezza del sistema di firma utilizzato.

I documenti firmati con la firma elettronica qualificata e con la firma digitale sul piano probatorio fanno piena prova di autenticità fino a querela di falso.

Per fare dei casi pratici la firma elettronica semplice è uno strumento concepito per regolamentare le transazioni commerciali tipiche dell'e-commerce (ad esempio un pagamento effettuato on line mediante una carta di credito), ed è idonea a far acquistare al documento informatico su cui è apposta il valore di forma scritta, oppure se non c'è documento informatico su cui apporre firma, si dà analogo valore all'operazione svolta (ad esempio quando digitiamo il codice Pin allo sportello bancomat, oppure quando ci vengono richieste credenziali, quali l'identificativo utente e la password, per accedere alle caselle di posta elettronica): spetta al giudice di volta in volta esprimere un giudizio sul valore probatorio di un documento sottoscritto con una firma elettronica semplice. La firma elettronica si associa solamente al documento (o all'operazione) cui è apposta, restando quindi sempre un elemento distinto da questo.

Lo stesso discorso vale per la firma elettronica avanzata che analogamente a quella semplice non ha riferimenti tecnologici univoci e chiaramente delineati: per questo motivo se da una parte esiste la massima libertà da parte degli operatori per implementare praticamente questi tipi di firma, dall'altra l'affidabilità di entrambe è direttamente conseguente al contesto in cui vengono utilizzate e alle soluzioni tecnologiche a cui si ricorre ed è questo il motivo per cui viene demandato al giudice il compito di valutarne l'efficacia e il valore probatorio.

Per quanto riguarda la firma elettronica avanzata la si può definire come una firma elettronica con alcune caratteristiche di sicurezza aggiuntive. Questo è il caso quando, in una transazione economica via internet non ci viene chiesto solo il PIN del bancomat ma ci viene anche richiesto un codice aggiuntivo generato da un dispositivo terzo, che può essere un telefono cellulare o altro dispositivo simile, che rafforza la sicurezza dell'operazione; ciò significa che se non si ha con sé lo strumento che genera il codice aggiuntivo il PIN da solo, che pure per le operazioni a sportello basta, non è sufficiente per concludere quella particolare transazione.

Si tratta quindi, nel caso della firma semplice e di quella avanzata, di due specifici tipi di firma utili tra privati che hanno come caratteristica quella di una assoluta libertà tecnologica lasciata agli sviluppatori e all'assenza di qualsiasi controllo

preventivo da parte della preposta autorità di vigilanza (dunque i soggetti che erogano sistemi di firma elettronica avanzata non sono soggetti ad alcuna registrazione). E' la prassi, per così dire, cioè il fatto che la maggior parte delle persone utilizzi questi metodi di firma elettronica semplice ed avanzata con effettivo beneficio e vantaggio, mantenendo nel contempo un elevato grado di sicurezza dei propri dati, ad avere sviluppato e diffuso questi 2 metodi.

Tuttavia le firme elettroniche avanzate hanno un valore limitato al solo contesto in cui vengono utilizzate (tra il sottoscrittore e il soggetto che offre il servizio di firma), rendendo quindi necessario che le loro condizioni di utilizzo siano preventivamente accettate per iscritto dagli utenti. E' il caso, nelle transazioni su internet, del segno di spunta (il cosiddetto flag) che l'utente è costretto a spuntare per poter procedere con la transazione: in questo modo, il soggetto che realizza la soluzione di firma elettronica avanzata si garantisce circa il fatto di avere informato gli utenti in merito agli esatti termini e condizioni relativi al servizio, compresa ogni eventuale limitazione dell'uso, sebbene poi nella realtà dei fatti quasi nessun utente vada effettivamente a leggersi i termini e le condizioni relative al servizio.

Per completare efficacemente un reale processo di FEA (firma elettronica avanzata) sarebbe necessario l'obbligo di identificare in modo certo l'utente tramite un valido documento di riconoscimento conservando copia dei documenti di riconoscimento e della dichiarazione di accettazione delle condizioni d'uso relativi a ogni utente per almeno venti anni. Inoltre, è di estrema importanza che tutte le fasi del processo siano correttamente registrate e che i relativi log file siano conservati insieme ai documenti e a tutte le altre informazioni relative al processo di firma elettronica. Quest'ultima fase spesso manca e per questo se da un punto di vista tecnico si può facilmente distinguere una firma elettronica semplice da una avanzata (il PIN del bancomat per le operazioni allo sportello e il PIN del bancomat più il codice di uno strumento terzo per le operazioni su internet), da un punto di vista normativo la differenza è più ardua da individuare.

Come ricordato la firma avanzata è stata probabilmente introdotta per semplificare la vita alle banche e agli operatori economici e commerciali che

hanno necessità di identificare chi compie una certa operazione ma possono procedere a questa verifica senza dover ricorrere ad un certificato rilasciato da un ente terzo ed a un dispositivo sicuro come è necessario per la FQ e la FD.

### **La firma digitale ed il suo funzionamento tecnico**

Con specifico riferimento al suo valore probatorio, il documento informatico dotato di firma digitale soddisfa pienamente il requisito della forma scritta anche quando questa è richiesta a pena di nullità, come nelle ipotesi previste dai numeri da 1 a 12 dell'art. 1350 c.c.

Il documento su cui è apposta una firma digitale, inoltre, fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto, se colui contro il quale il documento è prodotto ne riconosce la sottoscrizione, ovvero se questo è legalmente considerato come riconosciuto (art. 2702 c.c.).

Quindi il documento firmato digitalmente si presume riconducibile al titolare del dispositivo di firma, a meno che quest'ultimo non fornisca prova contraria (sulla scorta di quanto previsto dall'art. 21, comma 2, del CAD): ciò in quanto il sistema di verifica della firma si basa comunque su un metodo sicuro, come quello delle doppie chiavi asimmetriche.

Tale sistema è fondato sull'uso di due chiavi diverse, una diretta per cifrare e una inversa per decifrare (ciò comporta che non è possibile decifrare il testo con la stessa chiave usata per cifrarlo), generate insieme nel corso di un unico procedimento e correlate univocamente: una delle due chiavi può essere resa pubblica (consentendo a chiunque di controllare che un messaggio provenga proprio dal titolare dell'altra chiave, quella privata, e che non sia stato alterato o contraffatto), mentre l'altra deve essere mantenuta segreta. Pur conoscendo una delle due chiavi, infatti, non c'è nessun modo di ricostruire l'altra.

Per evitare di cifrare e decifrare l'intero documento si ricorre alla cifratura solo di un brevissimo riassunto del documento stesso, la cosiddetta "impronta" del testo (hash) che restituisce una stringa di caratteri.

Infatti, se alla fine della procedura l'impronta che risulta dalla decifratura con la chiave pubblica del mittente è uguale a quella che si ottiene applicando la

funzione di hash al testo non cifrato (in chiaro), è certo che esso provenga effettivamente dal titolare della chiave pubblica e quindi che il documento non è stato alterato dopo la generazione della firma digitale.

La pubblicazione e il controllo delle chiavi avvengono accedendo ad appositi registri, ovviamente per via telematica, che devono essere correttamente tenuti e aggiornati da una terza parte fidata, gli enti certificatori, che hanno il compito di gestire il database delle chiavi pubbliche e dei relativi certificati delle chiavi, nonché la responsabilità di procedere alla previa identificazione del soggetto che richiede la certificazione.

L'insieme degli elementi che compongono tale processo si definisce “infrastruttura di chiave pubblica” e si articola nei soggetti che vi partecipano (firmatario, certificatore, destinatario), nelle modalità in cui ciascuno di essi assolve al proprio ruolo e nelle forme di utilizzazione delle tecnologie disponibili.

Per quanto riguarda l'utilizzo in concreto di un sistema di firma digitale, l'operazione di firma in sé non costituisce un'azione di particolare complessità. Tuttavia, nei casi in cui si renda necessaria la firma di molteplici documenti, è possibile ricorrere alle procedure automatiche di firma, che rendono più rapido il meccanismo di apposizione della firma digitale.

### **Il caso della firma automatica**

Il DPCM 22 febbraio 2013 fornisce una definizione precisa di firma automatica quale “*particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore, in assenza di presidio puntuale e continuo da parte di questo*” (art. 1 lett. r).

Con particolare riferimento all'effettivo funzionamento delle firme automatiche, occorre precisare che queste non vengono realizzate mediante l'utilizzo dei comuni dispositivi forniti dai certificatori (token usb o smart card), ma si ricorre a strumenti tecnologicamente più avanzati e in grado di gestire più velocemente una maggiore quantità di dati.

## **Il caso della firma da remoto**

Per quanto riguarda, le firme da remoto (*server side*), queste costituiscono una tipologia di firma elettronica avanzata o di firma digitale utilizzabile via web: la chiave privata del firmatario e il relativo certificato di firma vengono conservati da parte di un certificatore accreditato in un server remoto basato su un sistema specifico, presso un server remoto, all'interno di un HSM (dispositivo crittografico hardware). Il DPCM 22 febbraio 2013 all'art.1 lettera q) definisce la firma remota semplicemente come: “*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*”.

Si tratta di uno strumento utile al sottoscrittore “itinerante” ovvero che non usa sempre lo stesso dispositivo per apporre la firma ma lo fa collegandosi tramite internet al server di firma.

Il vantaggio principale della firma remota risiede nel fatto che non si ha bisogno di un dispositivo crittografico personale ma basta avere la possibilità di dialogare col server di firma.

La firma remota pur simile alla firma automatica se ne differenzia in quanto si svolge in modo interattivo, mentre l'automatica non necessita dell'intervento del sottoscrittore e inoltre la firma remota viene in genere apposta da utenti che si collegano al server attraverso internet mentre al server di firma automatica si accede solo attraverso una LAN.

## **La firma autografa elettronica: un caso speciale**

Accanto alle tipologie di firma già analizzate, è possibile considerare anche una particolare modalità di firma grafometrica come tipologia di firma a sé stante, per la quale già esiste un riconoscimento nel nostro codice civile. Infatti in presenza di determinati presupposti, essa può essere considerata una firma autografa applicata non su un documento cartaceo, ma applicata indissolubilmente a un documento informatico, a patto che quest'ultimo abbia i requisiti tipici previsti per garantire la forma scritta ai sensi degli articoli 20 e 21 del CAD.

A voler essere pignoli in effetti la firma autografa od olografa, ovvero scritta di proprio pugno, non è stata sempre e solo legata alla carta: per acquisire e

conservare i segni distintivi di ogni individuo si sono utilizzati lo scalpello e la pietra per lo scultore, il pennello e la tela per il pittore, e così via.

Tramite le nuove tecnologie digitali di acquisizione e conservazione è possibile rilevare e preservare nel tempo gli stessi elementi grafometrici (nel caso specifico un segno distintivo chiamato firma) preservati sulla/dalla carta.

Si tratta quindi di una firma che, opportunamente acquisita e legata al documento, al pari della sottoscrizione su carta potrà essere verificata qualora venga disconosciuta in giudizio, con tecniche molto simili a quelle attualmente utilizzate dai periti grafologici.

Nei casi pratici (ad esempio al ritiro di un pacco, alla firma di una bolla di accompagnamento, al disbrigo di pratiche alla posta eccetera), la **firma “autografa elettronica”** viene elaborata mediante l'utilizzo di una tavoletta grafica e di una penna speciale in grado di acquisire, con notevole precisione, i tratti specifici della firma. I tratti impressi sulla tavoletta dalla speciale penna vengono trasformati in dati informatici e immediatamente dopo la loro acquisizione, vengono cifrati e sostanzialmente “fusi” con il documento informatico che si intende sottoscrivere. Il processo di sottoscrizione si conclude con la memorizzazione di tutti i dati così elaborati su di un supporto in grado di preservarne la leggibilità nel tempo.

Qualora fosse necessario procedere alla verifica della firma (ad esempio a seguito di un disconoscimento della sottoscrizione avvenuto in giudizio) sarà possibile decriptare i dati biometrici e confrontarli con quelli raccolti in giudizio dal perito grafico incaricato, che effettuerà le proprie comparazioni secondo regole non dissimili da quelle utilizzate negli attuali processi di verifica di sottoscrizioni su carta.

Dalle considerazioni svolte dunque si evince come, a prescindere da quelle che sono le regole tecniche per le firme elettroniche avanzate, è comunque possibile reperire nel nostro ordinamento gli elementi giuridici a supporto della validità e dell'autonomia della firma autografa digitale o elettronica.

La firma grafometrica può essere quindi una valida risposta a molti dei problemi posti dalla digitalizzazione e dalla informatizzazione dei processi.

Sostanzialmente è uno strumento elettronico di tipo avanzato ma di facile uso, può essere rilevata in qualche secondo, ricorda molto da vicino la classica firma autografa: occorre registrarla tramite un dispositivo elettronico biometrico, che rileva i dati della calligrafia del firmatario, unici per ogni persona, ovvero ritmo e velocità con cui si scrive, pressione esercitata dalla mano sul pennino, l'accelerazione della scrittura, il movimento aereo della mano nel firmare.

E' importante che all'atto della firma sia associata una connettività per il transito veloce delle informazioni e un sistema di conservazione digitale, che garantisce autenticità, opponibilità, integrità e accessibilità ai documenti informatici.

La firma grafometrica racchiude molti vantaggi: autenticazione e certificazione della proprietà della firma, integrità del documento firmato, ottimizzazione del trattamento, archiviazione dei documenti firmati e risparmio sui costi.

La firma autografa digitale o elettronica è menzionata nel CAD all'art. 25 comma 2: “*l'autenticazione della firma elettronica, 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, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico*”.

La firma grafometrica si sta diffondendo rapidamente e ne è accettato l'uso nei contesti più disparati<sup>37</sup>, anche quelli considerati una volta più “delicati” come la sottoscrizione di atti notarili. A questo proposito è stato recentemente emanato il provvedimento n. 619 del 25 novembre 2015 dell'Autorità Garante per la protezione dei dati personali che ha dato il via libera all'utilizzo in via sperimentale anche in ambito notarile di un sistema di firma grafometrica.

---

<sup>37</sup> Cosa ben comprensibile data la estrema semplicità per l'utente che si limita sostanzialmente a firmare su una tavoletta elettronica nello stesso identico modo in cui firmava su carta il che soprattutto per persone anziane o che abbiano poca dimestichezza con l'informatica o che abbiano difficoltà a ricordare PIN o altri codici è un vantaggio non di poco conto.

## Casi in cui la firma elettronica può essere sostituita da altri strumenti (CIE, TS, CNS, SPID)

Il decreto del Ministero dell'Interno del 23 dicembre 2015 (emanato di concerto con il Ministero dell'economia e delle finanze e con il Ministero per la semplificazione e la pubblica amministrazione) fissa le modalità tecniche di emissione della carta d'identità elettronica (CIE).

Non entriamo nel merito delle innumerevoli critiche rivolte alla CIE

Qui notiamo che la CIE non è mai stata utilizzata come modalità per accedere in rete ai servizi delle Pubbliche Amministrazioni, come invece prevede il CAD. Ricordiamo anche che è stata cancellata la disposizione che ne prevedeva l'unificazione con la TS (Tessera sanitaria) e che quindi, ad oggi, continueremo ad avere due strumenti separati.

In questa sede, l'aspetto più interessante è quello che riguarda la CIE come strumento per l'accesso in rete ai servizi delle Pubbliche Amministrazioni dato che l'art. 64. del CAD dice che *“La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica.; in assenza di questi strumenti, sono ammesse anche altre modalità, a condizione che “consentano l'individuazione del soggetto che richiede il servizio”.*

Successivamente è stato introdotto in questo contesto SPID (Sistema Pubblico di Gestione dell'Identità Digitale) che comunque non cancella CIE e CNS dato che ancora il CAD afferma *“L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni”.*

Come si lega a questo l'introduzione dello SPID?

A parte alcune discrepanze dovute allo sfasamento dei tempi di emanazione delle varie norme<sup>38</sup> si prevede che il rilascio delle identità digitali avviene su domanda dell'interessato e la verifica dell'identità del soggetto può anche avvenire tramite

---

<sup>38</sup> Tra le modalità di verifica dell'identità personale per il rilascio della identità digitale, ovvero dello SPID non è riportata la CIE mentre si cita esplicitamente TS e CNS

*“identificazione informatica tramite documenti digitali di identità, validi ai sensi di legge, che prevedono il riconoscimento a vista del richiedente all'atto dell'attivazione, fra cui la tessera sanitaria-carta nazionale dei servizi (TS-CNS), CNS o carte ad essa conformi”.*

Non entriamo qui nel problema dei vari livelli di SPID e nel fatto che ai diversi servizi accessibili dovrà corrispondere un certo livello di sicurezza che presuppone il rilascio dello SPID con procedure diverse<sup>39</sup>, ma certamente si porrà il problema di stabilire a quale livello corrisponde lo SPID rilasciato con verifica dell'identità tramite CIE o TS o CNS sperando che il livello 3 non sia accessibile solo tramite il mercato con costi a carico del cittadino<sup>40</sup>

Riguardo alla validità delle istanze presentate online, dal punto di vista della sottoscrizione, non dovrebbero esserci dubbi.

L'art. 65 del CAD prevede che *“Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici sono valide:*

- a) se sottoscritte mediante la firma digitale o la firma elettronica qualificata, il cui certificato è rilasciato da un certificatore accreditato;*
- b) ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi;*
- c) ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2 (cioè SPID).*

*Continua affermando che “Le istanze e le dichiarazioni inviate o compilate su sito secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento.”*

Quindi l'uso di SPID, CIE o CNS può sostituire *in toto* la firma elettronica nella sottoscrizione di istanze alla PA (ma presumibilmente anche imprese private che aderiranno al sistema).

---

<sup>39</sup> Appendice A del Regolamento Attuativo;

<sup>40</sup> D'altronde il livello 3 richiede che il gestore delle identità digitali deve rendere disponibili sistemi di autenticazione informatica a due fattori, basati su certificati digitali

Questo anche perché il DPCM 22 febbraio 2013, che contiene le “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali”; chiarisce che *“La realizzazione di soluzioni di firma elettronica avanzata non è collegata ad alcun supporto tecnologico specifico*, e stabilisce soltanto le caratteristiche (invero piuttosto stringenti) <sup>41</sup> che la firma elettronica avanzata deve avere per essere valida.

D'altronde lo stesso DPCM prevede che *“L'utilizzo della Carta d'Identità Elettronica, della Carta Nazionale dei Servizi, del documento d'identità dei pubblici dipendenti (Mod. ATe), del passaporto elettronico e degli altri strumenti ad essi conformi sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata ai sensi delle presenti regole tecniche per i servizi e le attività di cui agli articoli 64 e 65 del codice.”*

Quindi l'utilizzo dei documenti di identità elettronici - oltre a permettere l'accesso in rete ai servizi costituisce già di per sé firma elettronica avanzata, per cui l'istanza presentata via web è assolutamente valida a tutti gli effetti, e quindi si considerano rispettati i requisiti sopra citati dell'art. 56.

Rimangono da chiarire diversi aspetti tecnici legati soprattutto al considerare CIE e CNS come dispositivi atti o meno a generare una firma elettronica e di che tipo e quale sia il livello SPID rilasciato tramite questi dispositivi, così come andrà chiarito se per il livello 3 il cittadino dovrà sostenere un costo dopo aver già pagato per ottenere la CIE o la CNS.

Non viene chiarito se l'accesso e la sottoscrizione online di un soggetto che ha ottenuto l'identità SPID senza avvalersi di un documento di identità digitale sia da ritenersi conforme alle normative ma si presume che una carta di identità analogica (che per molto tempo sarà presumibilmente la più facile e soprattutto la

---

<sup>41</sup> Art. 56: “*1. Le soluzioni di firma elettronica avanzata garantiscono: a) l'identificazione del firmatario del documento; b) la connessione univoca della firma al firmatario; c) il controllo esclusivo del firmatario del sistema di generazione della firma, ivi inclusi i dati biometrici eventualmente utilizzati per la generazione della firma medesima; d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma; e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto; f) l'individuazione del soggetto di cui all'art. 55, comma 2, lettera a); g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati; h) la connessione univoca della firma al documento sottoscritto.*”

più rapida da ottenere) possa a buon diritto rientrare tra “*gli altri strumenti ad essi conformi*” citati nel DPCM 22/2/2013, e quindi essere equiparata ai documenti di identità digitali.

Da quanto esposto si ricava ancora una volta l’idea di una connessione forte tra i vari strumenti a vario titolo connessi con l’identità digitale e la necessità di un coordinamento strettissimo tra le varie iniziative messe in cantiere dal Governo, in particolare l’ANR e l’identità digitale, nella speranza che l’Agid peraltro già oberata di molteplici incombenze riesca a far fronte, magari opportunamente potenziata, a tutti gli obblighi prescritti.

## **PEC e FIRMA ELETTRONICA nel processo telematico**

Una analisi approfondita dei problemi legati all’introduzione progressiva del processo telematico in tutti i rami della giurisdizione e degli strumenti necessari, porterebbe troppo lontano ed esula dallo scopo di questo lavoro. Tuttavia dato che parliamo di PEC e Firma elettronica può essere utile vedere come questi strumenti entrino nel processo telematico. Va rilevato che anche da questo punto di vista il passaggio dal processo “cartaceo” a quello “digitale” non solo non è un cammino lineare ma è fatto di brusche frenate, di conversioni a U e di improvvise accelerazioni, ma soprattutto è stato condito di una miriade di iniziative, probabilmente lodevoli nelle intenzioni ma scoordinate quando non in conflitto tra loro.

Va ricordato anzitutto che il CAD, sancisce l’applicabilità di quanto ivi normato alla amministrazione della Giustizia con qualche cautela di troppo<sup>42</sup>. D’altra parte lo stesso CAD prevede per la emanazione delle norme tecniche in materia di

---

<sup>42</sup> Nella formulazione attuale (*Le disposizioni del presente Codice si applicano altresì al processo civile e penale in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico*) la dicitura “salvo che non sia diversamente disposto crea diversi problemi in ordine alla individuazione della norma prevalente in caso di non compatibilità, che stando alla lettera della norma sembrerebbero essere sempre “*le disposizioni in materia di processo telematico*”.

L’art. 4 del D.L. n. 193 del 2009 stabilisce che l’applicazione al processo, sia civile che penale, dei principi previsti dal CAD debba avvenire attraverso apposite regole tecniche approvate con decreto del Ministro della Giustizia.

giustizia l'intervento diretto del relativo Ministero<sup>43</sup>. Questo ha imposto l'emanazione da parte del Ministero della Giustizia di normative ad hoc, che ovviamente non contraddicono il CAD ma estendono alla amministrazione della giustizia i procedimenti telematici. Senza entrare nel dettaglio dei diversi procedimenti che nel tempo si sono succeduti, si può affermare che la fonte primaria risulta ad oggi il DM. 21 febbraio 2011 n. 44 che non a caso recita *“Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione..”*

Anche questo DM, come tutti quelli che riguardano il mondo digitale, oltre a modifiche successive quasi sempre fatte a colpi di cancellazione o modifica di singole parole, ha avuto bisogno per entrare effettivamente in vigore di norme tecniche riferite all'art. 34 (*Specifiche tecniche*). Queste norme tecniche sono state emanate con il PROVVEDIMENTO 16 aprile 2014 del Ministero della Giustizia e poi con il Decreto 28 dicembre 2015 contenente ulteriori modifiche alle specifiche tecniche

D'altronde il PCT (Processo civile telematico) che è partito molto in anticipo rispetto al Processo Penale Telematico, era già disciplinato dal D.P.R. 13 febbraio 2001 n. 123, successivamente integrato dal D.M. 17 luglio 2008, e poi ancora dal citato DM. 21 febbraio 2011 n. 44.

Il PTT (Processo Tributario Telematico) dopo fasi di sperimentazione viene disciplinato dal Decreto Ministero Economia e finanze 23/12/2013 n° 163, mentre l'art.2 del D.L. n.210 del 30 dicembre 2015, convertito con modificazioni dalla L. 25 febbraio 2016, n. 21, ha indicato la data del 1° luglio 2016 per l'avvio a regime del Processo Amministrativo Telematico. Norme diverse come si vede per i diversi processi, ma che hanno evidentemente lo stesso fine e che tuttavia, per

---

<sup>43</sup> Il CAD prevede all'art. 71 che le regole tecniche per la materia processuale vengano dettate dal Ministro della giustizia, di concerto con il Ministro per la pubblica amministrazione e l'innovazione mentre per tutta la PA le regole tecniche vanno emanate con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione. Si tratta di una disposizione che è applicazione dell'art. 110 della Costituzione, che attribuisce direttamente al Ministro della giustizia l'organizzazione e il funzionamento dei servizi relativi alla giustizia.

essere state emanate in tempi anche molto diversi, non sempre si coordinano tra loro. Qui interessa analizzare cosa accade riguardo a PEC e firma elettronica.

Riguardo alla firma elettronica essa è ovviamente prevista in tutti i passaggi del procedimento giudiziario, dal deposito degli atti alla scrittura delle sentenze. Tuttavia talvolta, per cercare di semplificare il lavoro degli uffici si scende in dettagli tali da rendere contraddittorie alcune disposizioni. Ad esempio riferendoci al PCT accanto alla prescrizione dell'uso della firma digitale nel processo civile telematico la normativa prescrive anche i formati da utilizzare nel PCT, ossia il formato CADES e il formato PADES<sup>44</sup>. (In realtà esiste almeno un altro formato riconosciuto dal nostro Ordinamento, lo XADES, oltre a diverse altre possibilità di implementazione della firma elettronica)

L'uso del CADES e del PADES come unici formati idonei al deposito degli atti per via telematica è prescritto dal “Provvedimento 16 aprile 2014” che ha introdotto l'utilizzo del formato PADES nel processo civile telematico (antecedentemente l'unico formato di firma digitale utilizzabile nel PCT era il CADES). La cosa quanto meno curiosa è che Il D.P.C.M. 40/2016 contenente le regole e le specifiche tecniche per l'attuazione del processo amministrativo telematico prevede che tutte le parti, dovranno depositare i loro atti telematicamente, atti che dovranno essere sottoscritti digitalmente esclusivamente tramite firma “PADES” e non anche, come invece consentito per il processo civile telematico, con firma “CADES”. Quindi, prima solo CADES, poi CADES e PADES, poi solo PADES. Il tutto non sembra fatto proprio per facilitare la vita agli operatori della giustizia.

Non solo, accade pure che in molte delle norme citate ci sono riportate le definizioni del CAD prima delle modifiche che saranno introdotte dallo Schema DPCM 20/01/2016 il quale fa riferimento per tutte le definizioni al regolamento eIDAS. Che si dovrà fare allora per non correre il rischio di rendere obsolete quando non addirittura inutilizzabili normative anche molto recenti? Una soluzione sarà sicuramente trovata, magari con una riscrittura ad hoc dei commi interessati, ma la questione pone in luce la stretta interdipendenza tra le normative

---

<sup>44</sup> Non entriamo qui nel dettaglio dei due formati, diciamo solo che mentre il CADES richiede l'uso di programmi ad hoc, il PADES richiede solo la disponibilità di un lettore per file .pdf

e la necessità di scrivere provvedimenti specifici per l'amministrazione della Giustizia. Questo significa che anche la semplice abolizione di un comma o magari di una sola definizione o la modifica di una sola parola nella normativa generale può provocare una serie di conseguenze a cascata dall'esito non sempre prevedibile.

Per quanto attiene alla PEC, anche qui senza entrare nei dettagli delle procedure previste nei vari tipi di procedimento (amministrativo, tributario etc.) la tendenza è chiaramente quella di usare la PEC come strumento esclusivo ad esempio per il deposito degli atti. Un problema è che anche in questo caso le procedure differiscono notevolmente nei vari tipi di processo.

Nella normativa più recente, quella già citata riguardante il Processo Amministrativo Telematico il deposito degli atti è previsto esclusivamente a mezzo PEC, e atti e documenti dovranno essere inviati dalla PEC del professionista alla PEC della sede giudiziaria adita e solo nel caso in cui il deposito non possa effettuarsi tramite PEC (per ragioni tecniche o per la particolare dimensione del documento) ad esso potrà procedersi mediante "UPLOAD" attraverso il SIGA (Sistema Informativo della giustizia amministrativa) che prevede anche una interfaccia riservata al magistrato per le operazioni di sua competenza. Ben diversa la situazione nel PCT. In questo caso gli atti da depositare vanno redatti con un apposito software detto "redattore atti" che va acquisito sul mercato (ne esistono molte e diverse implementazioni). Questo software si rende necessario perché l'art. 14 del "Provvedimento 16 aprile 2014" prescrive l'inserimento di tutti i documenti da trasmettere alla Cancelleria del Tribunale all'interno di un unico file crittografato. Contrariamente a quanto il nome suggerisce non si tratta di un software per la scrittura di un atto, bensì per l'"imbustamento" di un atto già scritto e convertito in PDF e per la sottoscrizione con firma digitale.

Infine va sottolineato come la PEC svolga un ruolo fondamentale nei diversi tipi di notifica che sarà messo in evidenza nella analisi di alcune sentenze in proposito.

La PEC non piace a molti come mezzo di notifica di atti giudiziari, anche se vengono spesso messi in evidenza gli indubbi vantaggi in termini di spesa e di rapidità. Esiste anche la tendenza ad usare mezzi diversi che rendano meno probabile qualsiasi tipo di contenzioso, ad esempio in alcuni tipi di processo telematico il deposito degli atti non avviene già più tramite la PEC ma attraverso procedure disponibili sui diversi portali come il SIGA mentre rimane l'uso della PEC nelle relazioni tra le parti.

D'altronde la legittimità dell'uso della PEC, anche in contesti non espressamente previsti dalla normativa è stata più volte ribadita nelle sentenze, anche della Cassazione che secondo G. Negri<sup>45</sup> con la sentenza 16622 del 31/03/2016<sup>46</sup> “*La Corte di Cassazione sdogana a tutti gli effetti l'uso della Pec per le notifiche penali. E lo fa dando una lettura estensiva delle disposizioni contenute nel decreto «Cresci Italia»*”

---

<sup>45</sup> Per una analisi vedi all'indirizzo: <http://www.quotidianodiritto.ilsole24ore.com/art>

<sup>46</sup> Qui reperibile <http://www.italgiure.giustizia.it/xway>

## LA MARCA TEMPORALE<sup>47</sup>

Si tratta anche in questo caso di uno strumento informatico evoluto<sup>48</sup>. Tra quelli presi in esame in questo lavoro, si tratta dello strumento più semplice e di più facile comprensione<sup>49</sup>. Come dice la parola stessa si tratta di una marca informatica che si può associare ad un documento informatico garantendone la validazione temporale eventualmente opponibile a terzi (articolo 20 comma 3 CAD). Semplificando e sulla falsariga di quanto fatto per la PEC e la raccomandata A/R e per la sottoscrizione informatica e la firma, in questo caso specifico si possono paragonare le marche temporali alla data apposta in calce a un documento che, fino a prova contraria garantisce legalmente data della produzione del documento ovvero più specificamente una marca temporale si può assimilare al bollo postale che fa fede rispetto alla data di spedizione o ricezione di un invio postale. Nella pratica la marca temporale viene creata apponendo ad un documento la firma elettronica qualificata di un soggetto terzo, ovvero di un certificatore abilitato a fare questa operazione.

Una marca temporale può essere apposta a documenti elettronici non firmati digitalmente così come a documenti informatici firmati: in quest'ultimo caso la marca temporale garantirà la validità della firma anche quando i certificati associati a quella determinata firma di un determinato soggetto saranno scaduti.

La marca temporale è utile per coloro che debbano associare una validazione temporale a documenti digitali e non è vincolata alla firma elettronica; le marche non sono associate alla persona e non necessitano di documentazione firmata digitalmente per la loro apposizione.

---

<sup>47</sup> La definizione di marca temporale più recente è quella riportata nel DPCM 22 febbraio 2013: “*i) marca temporale: il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo;*”

Diciamo che qui intendiamo come marca temporale il risultato di un qualche procedimento informatico che serve a dare una validazione temporale ovvero ad apporre una data ed un'ora certa ad un documento informatico. Per una analisi più approfondita della questione dei vari termini usati in questo campo e della confusione per l'uso abbastanza indiscriminato e indifferenziato dei termini marca temporale, marcatura temporale, validazione temporale vedi: <http://www.altalex.com/documents/news/2012/10/10/art-2215bis-c-c-la-marcatura-temporale-e-la-marca-temporale>

<sup>49</sup> Il che non implica una equivalente semplicità informatica; vedi a questo proposito l'avviso dell'AgID sull'uso dei diversi algoritmi per la generazione della marca temporale: <http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche/avvisi>

Devono inoltre essere utilizzate da tutte le imprese che emettono fattura a Pubblica Amministrazione attraverso il sistema di fatturazione elettronica, assegnando ad ogni fattura digitale emessa una marca temporale per garantirne data ed ora di generazione e l'impossibilità di modifica.

La marca temporale assume particolare rilevanza nella questione della conservazione documentale e, ovviamente, in particolare per i documenti digitali. Infatti mentre una firma elettronica ha una validità temporale limitata (in genere 3 o 4 anni) e i relativi certificati possono essere sospesi o soppressi prima della scadenza, una marca temporale va conservata dal gestore per almeno 20 anni. L'apposizione di una marca temporale ad un documento firmato digitalmente, dà certezza sul momento in cui la firma è stata apposta e certifica, anche dopo la scadenza del certificato, che la firma era valida al momento della apposizione e questo anche dopo molti anni dall'apposizione della firma dato che la marca temporale su richiesta dell'utente va conservata per un periodo anche maggiore dei "canonici" 20 anni. Proprio questo periodo di conservazione obbligatoria particolarmente lungo rende la marca temporale adatta a siglare atti che debbono essere conservati obbligatoriamente solo per un periodo più breve. Questo è il caso ad esempio delle varie ricevute (accettazione, consegna etc.) relative alla PEC che il gestore di PEC non è tenuto a conservare dato che l'obbligo per il gestore (e per soli 30 mesi) riguarda soltanto il c.d. "log", utile per la ricostruzione delle ricevute, ma privo di ogni informazione relativa al contenuto del messaggio mentre la ricevuta "completa" di avvenuta consegna contiene, al proprio interno, l'intero messaggio inviato, compresi gli allegati. Tutto questo diventa particolarmente importante ad esempio nel caso della notifica telematica da parte degli avvocati<sup>50</sup>.

Proprio il lungo periodo obbligatorio di conservazione rende la marca temporale adatta ai procedimenti di conservazione, dato che anche se la normativa consente una gamma diversificata di strumenti per dare certezza temporale ai documenti da conservare (ad esempio riversando il documento in un "sistema di conservazione",

---

<sup>50</sup> <http://www.pergliavvocati.it/forum/viewtopic.php?f=2&t=124>

attraverso il "protocollo informatico, eseguendo, nel caso del PCT, un "deposito telematico) la marca temporale appare una delle forme più semplici da usare.

Oltre tutto la relativa semplicità della marca temporale permette di implementarla in modi diversi. Oltre all'apposizione di una firma digitale da parte di un certificatore abilitato a farlo esistono anche modalità diverse come ad esempio il servizio Data Certa Digitale di Postel<sup>51</sup> che avviene attraverso l'apposizione della cosiddetta EPCM (Electronic Postal Certification Mark), rilasciata da Poste Italiane secondo quanto previsto dall'Universal Postal Union, al documento informatico. In questo caso oltre alla garanzia della certezza dell'esistenza del documento in una data e un'ora opponibile a terzi, viene fornita anche la garanzia della autenticità, integrità, affidabilità, leggibilità e reperibilità nel tempo dato il documento viene memorizzato nel sistema di conservazione digitale Postel accreditato dall'Agenzia per l'Italia Digitale (il che conferma l'importanza della marca digitale nella questione della conservazione documentale).

---

<sup>51</sup> Società delle Poste Italiane che si occupa in dettaglio di certificazione e conservazione [www.postel.it/](http://www.postel.it/)

## Come eIDAS modifica PEC, firma elettronica e marca temporale

### Cosa è eIDAS

Il Regolamento in materia di identificazione elettronica e servizi fiduciari, per le transazioni elettroniche nel mercato interno è stato pubblicato nella Gazzetta Ufficiale europea del 28 agosto 2014 ed è in vigore dal 17 settembre. Ciononostante, la sua applicazione negli Stati membri sarà graduale, affinché possano avere il tempo per adeguare i propri servizi e legislazioni di riferimento. In particolare le regole per i servizi fiduciari cominceranno a essere applicate dal primo luglio 2016 mentre l'obbligo di riconoscimento reciproco delle identificazioni elettroniche si applicherà a partire dalla metà del 2018.

Il Regolamento norma una serie di questioni e permetterà ai cittadini, alle imprese e alle amministrazioni di usare strumenti di identificazione elettronica e servizi fiduciari per accedere ai servizi on line o gestire transazioni elettroniche (ad esempio firme e sigilli elettronici, validazioni temporali elettroniche, servizi di raccomandata elettronica e servizi di certificazione per l'autenticazione web).

Si tratta di materie già ampiamente normate nei singoli stati ma la vera rivoluzione si avrà per l'inedita creazione di un quadro tecnico-giuridico certo a livello comunitario, che permetterà l'interoperabilità di tutti i sistemi d'identificazione elettronica adottati dai singoli Stati UE. In particolare infatti il regolamento eIDAS all'articolo 1 *“fissa le condizioni a cui gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro”*.

All'atto della presentazione dell'eIDAS avvenuta in sede comunitaria il 14 ottobre 2014 sono stati illustrati i benefici che cittadini e imprese ne ricaveranno cioè (nella traduzione di quanto riportato, in inglese sul sito della Commissione Europea)

- I cittadini potranno effettuare transazioni elettroniche transfrontaliere sicure e sfruttare al meglio i propri diritti in tutta l'Unione Europea, dalla iscrizione in un'università straniera, all'accesso alle cartelle cliniche elettroniche.
- Chi si sposta in un altro Stato dell'UE potrà gestire questo passaggio e tutti gli altri aspetti amministrativi on line, facendo a meno della carta.
- Le imprese dovranno fare i conti con meno burocrazia. I guadagni potranno essere enormi e portare a una significativa riduzione dei costi, con un conseguente incremento dei profitti. Per le piccole e medie imprese può trattarsi dell'elemento chiave per passare dalla stagnazione alla espansione.
- Quando cittadini e imprese potranno usare le proprie identità elettroniche per accedere ai servizi on line, ci saranno meno preoccupazioni sulla sicurezza e la privacy.
- I servizi pubblici diventeranno più flessibili e convenienti, paragonabili a quelli del settore privato.
- Le amministrazioni pubbliche potranno risparmiare denaro dei contribuenti, riducendo gli oneri amministrativi; così facendo potranno fornire servizi migliori e più efficienti e semplificare i rapporti con gli utenti. Ci saranno anche ritorni dal punto di vista ambientale, poiché si viaggerà meno e si ridurrà il consumo della carta.

Il Regolamento rimpiazza, con gli aggiornamenti resi necessari dall'evoluzione tecnologica la Direttiva 1999/93/EC che è stata in vigore per 15 anni ed ha costituito la base per le legislazioni e le normative nazionali.

Una notazione curiosa è che il Regolamento eIDAS vale solo per gli Stati membri ma non per le istituzioni comunitarie che comunque si sono impegnate in varie maniere ad usare i sistemi di identificazione elettronica e ridurre rapidamente il ricorso al cartaceo.

Anzitutto va detto che trattandosi di Regolamento comunitario esso è immediatamente valido senza necessità di ratifica da parte degli stati membri. Inoltre, come spesso accade in materia, anche questo Regolamento ha avuto

bisogno di decreti attuativi. In dettaglio sono stati emanati e pubblicati sulla Gazzetta europea del 9 settembre 2015 ben 4 decreti attuativi cioè

REGOLAMENTO DI ESECUZIONE (UE) 2015/1501 DELLA COMMISSIONE dell'8 settembre 2015 relativo al quadro di interoperabilità di cui all'articolo 12, paragrafo 8, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno

REGOLAMENTO DI ESECUZIONE (UE) 2015/1502 DELLA COMMISSIONE dell'8 settembre 2015 relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno

DECISIONE DI ESECUZIONE (UE) 2015/1505 DELLA COMMISSIONE dell'8 settembre 2015 che stabilisce le specifiche tecniche e i formati relativi agli elenchi di fiducia di cui all'articolo 22, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno

DECISIONE DI ESECUZIONE (UE) 2015/1506 DELLA COMMISSIONE dell'8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno

Di questi 4 decreti sono rilevanti, ai nostri scopi

il 1501 ove si stabilisce l'insieme minimo di dati di identificazione personale che rappresentano un'unica persona fisica o giuridica,

il 1502 ove stabilisce i livelli di garanzia per i mezzi di identificazione elettronica rilasciati nell'ambito di un regime di identificazione elettronica (vengono stabiliti i livelli basso, significativo ed elevato e ne vengono riportate le specifiche),

il 1506 che stabilisce in dettaglio le specifiche relative ai formati delle firme elettroniche.

Qui interessa mettere in rilievo l'impatto che l'adozione del regolamento eIDAS avrà sulla normativa italiana riguardante firma elettronica, PEC e marche temporali, considerando che la portata di eIDAS è molto più ampia e coinvolge l'intero processo di digitalizzazione delle procedure burocratiche, dei rapporti tra imprese cittadini e PA e dei rapporti delle imprese tra loro.

### **Limiti nell'applicabilità di eIDAS e suo valore giuridico**

Come si è già detto eIDAS non ha bisogno di ratifica da parte dei singoli Stati dato che la sua natura lo rende immediatamente applicabile. A questo riguardo è stato sollevato più di un allarme perché il contrasto con le norme nazionali potrebbe portare a situazioni di difficile gestione giacché, secondo alcuni<sup>52</sup> se il CAD non si adeguà “*tutte le disposizioni del CAD in contrasto saranno comunque abrogate in modo implicito*”. Affermazioni come questa probabilmente rappresentano, a parere di chi scrive, una forzatura per due ordini di motivi:

a) eIDAS pone nella premessa ben 77 considerazioni alcune delle quali sono di carattere molto generale ed enunciano i principi cui il Regolamento si ispira; alcune di queste premesse al testo pongono in realtà diversi limiti alla applicabilità *in toto* delle norme riportate nei singoli Stati membri: ad esempio al punto 13 si afferma che “*È opportuno che gli Stati membri rimangano liberi di utilizzare o di introdurre mezzi propri di accesso ai servizi online, a fini di identificazione elettronica, e che possano decidere dell'eventuale partecipazione del settore privato nell'offerta di tali mezzi. È opportuno che gli Stati membri non abbiano l'obbligo di notificare i loro regimi di identificazione elettronica alla Commissione. Spetta agli Stati membri decidere se notificare alla Commissione tutti, alcuni o nessuno dei regimi di identificazione elettronica utilizzati a livello nazionale per l'accesso almeno ai servizi pubblici online o a servizi specifici*”.

---

<sup>52</sup> Vedi ad esempio <http://www.forumpa.it/pa-digitale/caccia -il-cad rischia-la-brogazione>

punto 21 delle premesse ribadisce che non è opportuno stabilire un “*obbligo generale*” a far uso dei servizi fiduciari e chiarisce che “*i sistemi istituiti in imprese o amministrazioni pubbliche per la gestione delle procedure interne che fanno uso di servizi fiduciari non dovrebbero essere soggetti ai requisiti previsti dal presente regolamento*”, il che, come si capisce, lascia un margine fin troppo ampio ai singoli Stati membri per limitare l’applicazione del Regolamento. Anche nel corpo del provvedimento alcune affermazioni vanno nel senso di garantire ai singoli paesi un margine di libertà (che sembra di nuovo fin troppo ampio) nella applicazione di eIDAS; ad esempio proprio l’art.2 (Ambito di applicazione) recita al comma 2 : “*Il presente regolamento non si applica alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell’ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti*”. Cosa poi si debba intendere per sistema chiuso resta tutto da decidere, ma non sarebbe contraddittorio con questa norma decidere che ad esempio tutto ciò che concerne lo svolgimento di un particolare tipo di processo, tributario o amministrativo che sia, costituisce un sistema chiuso e per ciò stesso in quel particolare sistema chiuso eIDAS non troverebbe applicazione. Non si tratta qui di andare a cercare cavilli per non applicare il Regolamento europeo, ma di capire che ci sono i margini per una applicazione fatta *cum grano salis* senza buttare a mare immediatamente tutto ciò che è stato fatto in Italia (spesso in anticipo sul resto d’Europa) in questo campo. Sembrano pertanto eccessive le preoccupazioni, da più parti espresse sui rivolgimenti epocali e sulle conseguenze negative che l’adozione del Regolamento eIDAS potrebbe provocare nei sistemi di recapito certificato e firme elettronica italiani.<sup>53</sup>

Il problema che si pone è, come spesso accade nei rapporti con l’Europa di natura diversa; non si tratta infatti di un problema solo giuridico, ma anche e soprattutto di tipo politico ed economico. Non è un caso l’art.1 ponga una premessa molto chiara; si afferma infatti che il regolamento fissa norme e condizioni “*Allo scopo di garantire il buon funzionamento del mercato interno perseguendo al contempo un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei*

---

<sup>53</sup>Per un approfondimento sulla natura fin troppo “prudente” del Regolamento eIDAS vedi ad esempio: <http://www.e-idas.org/eidas-regolamento-articolo-2/>

*servizi fiduciari*”. Anche in altri articoli si ribadisce l’importanza della “*libera circolazione nel mercato interno*”<sup>54</sup> Quindi lo scopo primario è garantire il buon funzionamento del mercato interno ed è ovvio che applicare nel modo più ampio eIDAS garantirebbe all’Italia la possibilità di sfruttare grandi opportunità economiche, sia perché il paese ha una buona esperienza nell’uso degli strumenti elettronici e quindi può proporre quegli strumenti a livello europeo, entrando quindi in un mercato molto più vasto di quello nazionale, sia perché l’adeguamento a eIDAS e alle procedure da esso previste potrebbe favorire l’arrivo di aziende e operatori europei nel mercato italiano.

b) il secondo aspetto che va considerato è che il CAD italiano è uno strumento rivolto *in primis* alla Pubblica Amministrazione ed è noto che in questo campo la potestà normativa dei singoli paesi è praticamente totale; di nuovo non si tratta tanto di un problema giuridico ma economico e politico. Infatti se è pur vero che l’Italia ha pieni poteri nel normare il funzionamento della macchina amministrativa pubblica è ancora più vero che molte imprese e imprenditori stranieri dicono di essere frenati dall’investire in Italia dalle lungaggini e complicazioni burocratiche. Quindi l’adeguamento ai principi di eIDAS può essere una occasione per semplificare procedure e normative con indubbi vantaggi economici.

Va anche messo in evidenza che viene estesa la possibilità di ricorrere a certificati di firma (e quindi a certificatori) anche provenienti da paesi non facenti parte della Unione Europea, purché siano rispettati certi requisiti, il che ci riporta all’esigenza di creare i presupposti perché il mercato italiano degli strumenti elettronici di firma e spedizione telematica sia messo in grado di competere senza essere gravato da impedimenti burocratici troppo forti<sup>55</sup>, visto che si tratta di competere non solo in Europa ma addirittura a livello globale.

---

<sup>54</sup> L’art. 4 si intitola non a caso “Principio del mercato interno”

<sup>55</sup> Ricordiamo la polemica, non ancora sopita sulla necessità di un capitale sociale molto elevato per entrare (o rimanere) nel campo della certificazione, polemica nata dalla equiparazione fatta nello Schema DL 20/01/2016 delle società di certificazione alle società di capitali con la conseguenza di dover disporre di un capitale sociale di 5 milioni di euro che appare eccessivo e comunque penalizzante rispetto alle tante società di medie dimensioni che già operano sul mercato, come peraltro messo in rilievo anche dal Consiglio di Stato nel suo parere.

Va detto che, essendo la normativa europea prevalente rispetto a quella nazionale, eventuali incompatibilità tra le due sono risolte in favore della normativa europea<sup>56</sup>. Tuttavia deve essere posta la massima attenzione perché le incompatibilità siano eliminate con una adeguata modifica della normativa nazionale per evitare contenziosi che, seppur risolti in partenza dal punto di vista astratto, possono risultare molto pericolosi. La profonda modifica del CAD, chesi cerca di fare con lo SCHEMA DL 20/01/2016 tende, tra gli altri, anche a questo scopo, anche se da più parti si è sottolineato come solo una riscrittura ex novo del CAD avrebbe, probabilmente evitato ogni possibile incompatibilità tra le norme comunitarie e quelle nazionali<sup>57</sup>.

Prima di affrontare l'analisi dei cambiamenti introdotti da eIDAS bisogna ricordare che eIDAS introduce in termini generali la nozioni di Servizi fiduciari (Trusted Services)

Con il termine servizio fiduciario si indica un insieme di servizi elettronici, forniti in genere a pagamento, caratterizzati da:

- i. creazione, verifica e convalida di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato, certificati relativi a tali servizi;
- ii. creazione, verifica e convalida di certificati di autenticazione di siti web;
- iii. conservazione di firme, sigilli o certificati elettronici relativi a tali servizi.

Un servizio fiduciario viene detto “qualificato se soddisfa i requisiti stabiliti dal Regolamento eIDAS e fornisce garanzie superiori in termini di sicurezza e qualità del servizio”. ed è sottoposto a vigilanza da un apposito organismo nazionale (l’Agenzia per l’Italia Digitale in Italia). Il concetto di servizio fiduciario qualificato comprende i certificatori accreditati (che rilasciano le smart card per la firma digitale), i conservatori accreditati e gestori di posta elettronica certificata già presenti in Italia. Ci sono però alcune differenze importanti rispetto al regime vigente basato sulla Direttiva Europea 1999/93/EC abrogata da eIDAS. (Proprio

---

<sup>56</sup> Nei limiti ricordati nel paragrafo precedente della applicabilità e della effettiva applicazione negli Stati membri delle disposizioni del Regolamento.

<sup>57</sup> <http://www.forumpa.it/pa-digitale/il-cad-che-ho-letto-e-il-cad-che-sognavo>  
<http://www.agendadigitale.eu/identita-digitale/che-restera-del-cad>

per dare modo ai singoli paesi di adeguarsi alle nuove norme e soprattutto di trasferire nella nuova cornice certificazioni e accreditamenti stabiliti in base alla direttiva abrogata eIDAS detta disposizioni transitorie)<sup>58</sup> Anzitutto il termine “accreditamento” è stato sostituito da “qualificazione” (il vecchio termine potrebbe creare confusione con le operazioni di accreditamento di organismi di certificazione, svolte da un ente di accreditamento riconosciuto (in Italia si tratta di Accredia). Rimane la funzione di vigilanza e si introduce l’obbligo per i prestatori di servizi fiduciari di essere sottoposti a valutazioni di conformità da parte di idonei soggetti terzi (a loro volta accreditati da un ente di accreditamento riconosciuto).

### Modifiche riguardo alla PEC

Negli stati membri dell’UE sono presenti diversi sistemi simili alla PEC italiana ma i diversi sistemi non sono interoperabili tra loro. eIDAS prova a colmare questa lacuna introducendo in tutti gli stati i servizi identificati in inglese come Registered Electronic Delivery (RED).

Questi servizi si affiancano ai sistemi nazionali ma inevitabilmente in tempi non troppo lunghi i sistemi nazionali dovranno diventare tutti conformi al modello RED, in vista soprattutto del reciproco riconoscimento e dell’obiettivo esplicitamente dichiarato da eIDAS di favorire scambi e interazioni tra gli stati.

eIDAS definisce i servizi elettronici di recapito certificato come “*un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;*”

I servizi di recapito per essere qualificati devono rispondere ai requisiti riportati nell’articolo 44 di eIDAS che recita:

*I servizi elettronici di recapito certificato qualificati soddisfano i requisiti seguenti:*

---

<sup>58</sup> Art.51:Disposizioni transitorie

- a) sono forniti da uno o più prestatori di servizi fiduciari qualificati;
- b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente;
- c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati;
- d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;
- e) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;
- f) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata

Viene ribadito che i servizi elettronici di recapito certificato hanno pieno effetto giuridico negli Stati membri della UE. Infatti l'articolo 43 dell'eIDAS recita:

1. *Ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato.*
2. *I dati inviati e ricevuti mediante servizio elettronico di recapito certificato qualificato godono della presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate nel servizio elettronico di recapito certificato qualificato.*

Quindi i servizi RED e la PEC si assomigliano, ma non sono esattamente la stessa cosa, per cui sarà necessario modificare alcune delle regole tecniche della PEC per renderla conforme a quanto stabilito da eIDAS. In particolare il primo requisito che necessita è un elevato livello di sicurezza nell'identificazione del mittente. La regola per individuare un livello di garanzia elevato sta nell'articolo 8, paragrafo 2, lettera c) e nel già citato Regolamento di esecuzione 2015/1502

Il servizio RED garantisce l'identificazione del destinatario prima della trasmissione dei dati (lettera c art. 44) e a questo si dovrà uniformare la PEC. Anche le lettere d) e) del medesimo articolo richiedono caratteristiche che potranno essere rispettate con qualche aggiustamento al sistema delle ricevute PEC, dato che prevedono per l'invio e la ricezione dei dati la garanzia di una firma elettronica avanzata e un di sigillo elettronico avanzato ad oggi non contemplati nella normativa sulla PEC. Infine alla lettera f) si richiede che gli elementi temporali dei servizi RED devono utilizzare meccanismi di validazione temporale elettronica qualificata ed anche questa caratteristica dovrà essere oggetto di aggiustamento delle norme tecniche sulla PEC.

Si può certo concludere che senza sforzi eccessivi e con alcuni aggiustamenti la PEC può diventare conforme a quanto stabilito da eIDAS e quindi il patrimonio di competenze e capacità tecniche e organizzative cresciuto in questi anni attorno alla PEC non andrebbe perduto nell'adeguamento alla normativa europea.

Rimangono ancora voci che chiedono l'abolizione tout court della PEC giudicata troppo complessa e non abbastanza flessibile per adeguarsi alla evoluzione tecnologica e ai cambiamenti nei rapporti tra PA imprese e cittadini, ma sembra di poter dire che l'adozione di eIDAS, da qualcuno vista come il de profundis della PEC in realtà in qualche modo rivitalizzi la PEC, a patto ovviamente di cogliere l'occasione per le modifiche e gli aggiustamenti necessari e probabilmente la prima cosa da fare è rivedere la tendenza ad introdurre specifiche diverse per i diversi usi che della PEC si fanno.<sup>59</sup>

### **Modifiche riguardo alla Firma Elettronica**

Viene stabilita in eIDAS la piena validità giuridica della firma elettronica e viene stabilito che una firma elettronica qualificata rilasciata in uno stato membro deve essere riconosciuta in tutta l'Unione. Infatti all'articolo 25 eIDAS recita:

*1.A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua*

---

<sup>59</sup> Nel capitolo sulla PEC si sono evidenziate le (inutili) specificazioni che della PEC si fanno ogni volta che se ne configuri l'obbligatorietà in un determinato procedimento

*forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.*

*2.Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.*

*3.Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.*

Si tratta di una disposizione che nella sua semplicità introduce una novità importantissima poiché non sarà possibile, per nessuno stato membro, disconoscere la validità di una firma elettronica apposta in un altro Stato (ovviamente se conforme agli standard stabiliti in eIDAS).

Nello stesso solco si inserisce quanto stabilito all'articolo 27 che riguarda le firme elettroniche nei servizi pubblici e che afferma l'obbligo di riconoscere in questo particolare settore la validità della firma elettronica avanzata e di non richiedere **per un utilizzo transfrontaliero** livelli di garanzia di sicurezza più elevati di quelli della firma elettronica qualificata.

Anche questa norma, apparentemente quasi banale è destinata ad incidere fortemente sui rapporti con le Pubbliche Amministrazioni dei vari stati membri, che notoriamente sono le istanze in cui maggiori sono le resistenze al cambiamento. Purtroppo va rilevato che nelle premesse, si stabilisce un principio che contrasta con la volontà più volte ribadita di rendere interoperabili i vari sistemi. Infatti il punto 23 delle premesse recita: “*Nella misura in cui il presente regolamento disponga l'obbligo di riconoscere un servizio fiduciario, tale servizio fiduciario può essere rifiutato solo qualora il destinatario dell'obbligo non sia in grado di leggerlo o verificarlo per motivi tecnici che sfuggono al suo immediato controllo. Tuttavia, tale obbligo non dovrebbe di per se stesso esigere che un organismo pubblico ottenga l'hardware e il software necessari per la leggibilità tecnica di tutti i servizi fiduciari esistenti*”.

Ora è chiaro che se un organismo pubblico non è tenuto a dotarsi del software necessario per la leggibilità di un servizio fiduciario sembra piuttosto improbabile che possa riconoscerne la validità. L'unica speranza in questo caso, per evitare scappatoie, è che tutti i

servizi fiduciari operino con modalità tecniche tali da non necessitare di software particolari per decifrare messaggi e documenti.

La prima grande differenza tra il CAD e eIDAS è che nel regolamento europeo sono disciplinate solamente tre delle tipologie di firma elettronica individuate dal CAD (firma elettronica, avanzata e qualificata) insieme a tre sigilli elettronici (ripartiti allo stesso modo). La firma digitale propriamente detta resterebbe dunque una peculiarità della normativa italiana.

Diversa, anche se, ovviamente solo in parte, la definizione di firma elettronica nel Regolamento europeo. Questa viene infatti descritta come “*dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare*”. Questo significa che mentre nel CAD viene messa in risalto la funzione identificativa della firma , in eIDAS viene messa in risalto la sua funzione dichiarativa: la firma elettronica è usata essenzialmente dal firmatario “per firmare” e quindi per esprimere la propria adesione al contenuto del documento informatico firmato, mentre rimane sullo sfondo la funzione identificativa.

Un novità di rilievo di eIDAS in qualche modo connessa con la firma elettronica è l'introduzione dei sigilli elettronici (elettronico, avanzato e qualificato), definiti dal Regolamento eIDAS come “*dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi*”. Il certificato qualificato di sigillo elettronico dovrà possedere gli stessi requisiti del certificato di firma elettronica qualificata, ma anziché ad una persona fisica sarà riferito ad una persona giuridica. Possiamo quindi pensare al sigillo elettronico come a un timbro virtuale utile ad assicurare l'integrità e la correttezza dell'origine dei dati del documento informatico su cui è apposto e la provenienza da una specifica persona giuridica.

Alcuni degli aspetti più strettamente tecnici riguardanti le modalità pratiche di attuazione della firma elettronica o i dispositivi per la creazione di firme elettroniche qualificate o i requisiti per la convalida delle firme elettroniche qualificate sono dati in eIDAS in forma abbastanza generica da essere, come si dice, **tecnologicamente neutri** ovvero non riconducibili a specifiche procedure

informatiche o a specifiche tecnologie. Si tratta di un principio rispettato in tutto il Regolamento, principio assolutamente necessario se non si vuole rendere obsoleta la normativa in tempi brevissimi.

### **Modifiche riguardo alla Marca Temporale**

Sostanzialmente la struttura della marca temporale rimane immutata anche se il Regolamento eIDAS la definisce con maggiore precisione (parlando però di validazione e non di marca) come "*dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento*"

Anche in questo caso l'elemento di maggiore novità e impatto è il riconoscimento degli effetti giuridici e l'estensione a tutti gli stati membri di questo riconoscimento. Infatti l'articolo 41, in modo del tutto analogo a quanto fatto per la firma elettronica recita: "*3. Una validazione temporale elettronica rilasciata in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli Stati membri.*".

Un aspetto molto rilevante riguardo alla marca temporale è quello che si ricava dalla lettura dell'art.42 (Requisiti per la validazione temporale elettronica qualificata) Infatti al comma 1 di questo articolo si stabilisce che: "*1. Una validazione temporale elettronica qualificata soddisfa i requisiti seguenti: a) collega la data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati; b) si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato; e c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.*". Il punto c) desta alla prima qualche perplessità: infatti se la validazione temporale viene apposta tramite firma elettronica o sigillo elettronico non è chiaro cosa è che la differenzia di fatto da questi due strumenti. Ma una analisi più attenta ci dice che la firma e il sigillo che di fatto costituiscono validazione temporale appartengono non alla persona fisica o giuridica che hanno interesse a validare l'atto ma al certificatore che si assume l'onere di certificare data e ora del documento. La marca temporale e la validazione temporale,

sembrano scontare anche in questo contesto europeo una sorta di vizio di origine dato che, se firma e sigillo avanzati (del prestatore di servizi fiduciari) costituiscono mezzo valido per la validazione temporale, non è chiaro per quale motivo non possano essere usate quelle di chi è interessato a validare l'atto e debba invece scomodarsi il prestatore di servizi in prima persona. Messa nei termini in cui eIDAS tratta la validazione temporale sembra proprio che, essendo la validazione temporale, di fatto, compresa nella firma e sigillo elettronico, così come viene configurata, appare quasi superflua o quantomeno si potrebbe facilmente pensare a meccanismi che la rendano tale<sup>60</sup>. A questo proposito qualcuno sostiene che con eIDAS la marca temporale italiana muore. In realtà non è esattamente così ed è proprio l'art.42 a soccorrerli, laddove parla, come metodo per la validazione temporale, oltre che di firma e sigillo, anche di “*un metodo equivalente*” e la marca temporale italiana potrebbe benissimo rientrare in questa fattispecie, così come possono rientrarvi altri metodi come DataCerta di Postel. Rimane comunque l'esigenza di una maggiore chiarezza e semplicità che proprio nello specifico caso della validazione temporale eIDAS pare non possedere del tutto.

Inoltre va considerato il ruolo fondamentale della marca temporale nella questione della conservazione dei documenti digitali<sup>61</sup> tenuto conto dei differenti tempi di validità dei diversi strumenti elettronici.

### eIDAS e il sigillo elettronico

Un novità di rilievo di eIDAS in qualche modo connessa con la firma elettronica è l'introduzione dei sigilli elettronici (elettronico, avanzato e qualificato), definiti dal Regolamento eIDAS come “*dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi*”. Il certificato qualificato di sigillo elettronico dovrà possedere gli stessi requisiti del certificato di firma elettronica qualificata, ma anziché ad una persona fisica sarà riferito ad una persona giuridica. Possiamo quindi pensare al sigillo elettronico come a un timbro virtuale

---

<sup>60</sup> L'uso della PEC di fatto contiene e sostituisce una marca temporale, anche se questa si riferisce al messaggio di PEC e non al documento contenuto.

<sup>61</sup> Vedi il paragrafo specificamente dedicato alla MT in questo lavoro

utile ad assicurare l'integrità e la correttezza dell'origine dei dati del documento informatico su cui è apposto. In qualche modo si può dire che si tratta della firma elettronica delle persone giuridiche.

Gli aspetti del sigillo elettronico sono trattati in modo identico a quanto fatto per la firma elettronica (il regolamento dice che al sigillo elettronico si applicano *mutatis mutandis* gli stessi articoli che si applicano (riguardo ai dispositivi, alla convalida, alla conservazione) alla firma elettronica

In modo del tutto analogo a quanto fatto per la firma elettronica, si stabilisce il valore probatorio e il riconoscimento interstatale del sigillo elettronico laddove l'art.35 recita:

1. *A un sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati.*
2. *Un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato.*
3. *Un sigillo elettronico qualificato basato su un certificato qualificato rilasciato in uno Stato membro è riconosciuto quale sigillo elettronico qualificato in tutti gli altri Stati membri.*

Possiamo concludere questo capitolo dicendo il Regolamento eIDAS rappresenta indubbiamente una novità di grande portata poiché stabilisce diversi principi che avranno un forte impatto sulla regolamentazione degli strumenti che qui stiamo analizzando ed una loro diffusione e integrazione a livello europeo.

Riconoscimento reciproco e neutralità tecnologica sono indubbiamente tra i principi fondamentali stabiliti da eIDAS.

Un'ultima notazione su eIDAS. Il Regolamento pone l'enfasi assai più sulla certificazione che sulla definizione degli strumenti in sé. Infatti requisiti per la certificazione sono dettati in modo molto stringente negli Allegati I, II, III del Regolamento mentre firme, sigilli e recapito elettronico sono definiti in modo più

generico. Proprio questo, assieme al principio della **neutralità tecnologica** permette di ipotizzare che per rendere conformi alla normativa europea gli strumenti elettronici utilizzati in Italia e qui analizzati non ci dovrebbe essere necessità di cambiamenti radicali nella normativa italiana. Purtroppo (o per fortuna) i cambiamenti tecnologici sono così rapidi che probabilmente eIDAS avrà vita più breve della Direttiva che l'ha preceduto anche se è da apprezzare lo sforzo per la creazione di un quadro comune europeo che sicuramente avrà importanti ricadute di vario tipo sulla vita quotidiana dei cittadini europei.

## Come il nuovo CAD modifica PEC, firma elettronica e marca temporale

### Cosa intendiamo per nuovo CAD

Con il termine Codice dell'Amministrazione Digitale (CAD), si intende il D. Lgs. 7 marzo 2005, n. 82, entrato in vigore il 1º gennaio 2006. Si tratta di un corpo organico di disposizioni relativo all'uso delle tecnologie informatiche nella PA che stabilisce una serie di norme e un quadro legislativo entro cui deve attuarsi la digitalizzazione dell'azione amministrativa e sancisce i diritti dei cittadini e delle imprese in materia di uso delle tecnologie nei rapporti con le Amministrazioni. Si tratta di normative che volevano avere un carattere di quadro e che hanno avuto bisogno di numerosi decreti attuativi e di norme tecniche anche piuttosto complesse. Il CAD è stato ripetutamente modificato, anche in modo sostanziale tanto che in diverse occasioni si è parlato di nuovo CAD, in particolare in occasione della promulgazione del decreto legislativo n. 235 del 2010 e delle relative Regole tecniche arrivate solo tre anni più tardi (DPCM 117 del 21 maggio 2013)

Per capire la mole di modifiche e integrazioni intervenute successivamente basta ricordare che nel sito [www.normattiva.it](http://www.normattiva.it) sono elencate qualcosa come un centinaio di modifiche<sup>62</sup> al testo originale.

Qui intendiamo analizzare quali cambiamenti sono stati apportati alla firma elettronica, alla PEC e alla marca temporale dall'ultima importante norma di modifica del CAD cioè lo SCHEMA DI DECRETO LEGISLATIVO RECANTE MODIFICHE E INTEGRAZIONI AL CODICE DELL'AMMINISTRAZIONE DIGITALE DI CUI AL DECRETO LEGISLATIVO 7 MARZO 2005, N. 82, AI SENSI DELL'ARTICOLO 1 DELLA LEGGE 7 AGOSTO 2015, N. 124, IN MATERIA DI RIORGANIZZAZIONE DELLE AMMINISTRAZIONI PUBBLICHE approvato dal Consiglio dei ministri in attuazione di una legge delega volta a rendere operativa una ampia riforma della PA.

---

<sup>62</sup>[http://www.normattiva.it/do/atto/vediAggiornamentiAllAtto?atto.dataPubblicazioneGazzetta=2005-05-16&atto.codiceRedazionale=005G0104&currentSearch=ricerca\\_semplice](http://www.normattiva.it/do/atto/vediAggiornamentiAllAtto?atto.dataPubblicazioneGazzetta=2005-05-16&atto.codiceRedazionale=005G0104&currentSearch=ricerca_semplice)

Come già detto il Decreto Legislativo non è ancora noto nella sua forma definitiva, anche se il Governo pare orientato a non fare modifiche sostanziali. Tuttavia dato che prima della emanazione definitiva sono previsti diversi passaggi che potrebbero, almeno in linea teorica apportare modifiche, ci atterremo nella trattazione che segue alla analisi dei principi generali e di quelle disposizioni che, essendo tra le meno controverse, rimarranno sicuramente inalterate nella versione finale.<sup>63</sup>

Va detto che, anche in questa occasione, abbiamo a che fare con un decreto che modifica il CAD del 2005, in parte in conseguenza di normative successive al CAD stesso (in particolare il Regolamento eIDAS), in parte a seguito di cambiamenti intervenuti nelle tecnologie sottostanti gli strumenti elettronici in esame. Se si tiene conto che già nel 2010, al momento dell'approvazione del decreto legislativo 235/2010 si parlava esplicitamente di nuovo CAD, e che oggi riferendosi alla rilevanza delle modifiche apportate si parla ancora di nuovo CAD, si può ben capire come possa diventare arduo districarsi nell'insieme delle norme che disciplinano questa materia e come il tutto possa anche influenzare i pronunciamenti dei tribunali in caso di contenzioso, dovendosi fare la massima attenzione al momento in cui i fatti sono avvenuti, onde individuare la norma che *in quell'esatto momento* era vigente.

Inoltre la forma in cui è scritto tutto il Decreto in esame rende problematico comprenderne l'esatta portata.

Il decreto legislativo è composto da 65 articoli che sono tutti di modifica o abrogazione di articoli del CAD 2005 (ben 27 ne vengono soppressi con il solo articolo 64 non a caso intitolato abrogazioni), modifica di commi o di parti del singolo comma o addirittura modifica o sostituzione di singole parole (“certificatori” diventa quasi ovunque, ma probabilmente non dappertutto “prestatori”) e persino modifiche ai riferimenti normativi. Che poi all’art. 3 dopo un comma già chiamato 1ter (perché evidentemente frutto di modifiche successive all’approvazione del CAD), si aggiunga un comma 1quater, 1quinquies, 1sexties

---

<sup>63</sup> Bisogna ricordare che tra i pareri, obbligatori ma non vincolanti, quello del Consiglio di Stato è stato particolarmente severo nei confronti dello Schema di DPCM. Per un’analisi di quanto evidenziato dal Consiglio di Stato vedi [http://www.agendadigitale.eu/egov/cad-ripensare-la-riforma-pa-ecco-tutti-i-punti-critici\\_2133.htm](http://www.agendadigitale.eu/egov/cad-ripensare-la-riforma-pa-ecco-tutti-i-punti-critici_2133.htm)

non sembra il modo migliore per avere una normativa chiara e accessibile. Tutto questo per dire che è davvero difficile capire cosa esattamente dica, nel dettaglio, il nuovo CAD una volta fatto il certosino lavoro di *taglia, copia, incolla, modifica..* Infatti il lavoro di sostituzione e modifica del testo originario per ottenere il testo vigente è molto impegnativo ma è d'altra parte assolutamente necessario per valutare in modo analitico la portata della nuova normativa. (alcuni tentativi sono stati fatti mettendo in rete versioni che riportano il testo originale e quello risultante dalle modifiche. Particolarmente utile è quanto riportato in <https://docs.google.com/document/d/16f>

La cosa è ancora più complessa se si considera l'iter che il decreto delegato deve compiere e tutti i pareri che diversi organi devono esprimere, i quali possono portare a modifiche con tutta probabilità non di sostanza ma magari solo finalizzate a rimediare a qualche svista o incongruenza. Ma, come abbiamo cercato di dire più volte, stiamo parlando di un campo in cui davvero *il diavolo si nasconde nei dettagli*. Peraltro è probabile che il governo vorrà limitare al massimo eventuali modifiche, anche ammesso che modifiche ce ne siano, non fosse altro che per lo scarso tempo a disposizione considerato che l'entrata in vigore del decreto è stabilita a luglio 2016 in concomitanza con Eidas. Per questo le analisi che seguono si concentreranno sugli aspetti di carattere più generale che, con tutta probabilità, anche in presenza di modifiche successive, non dovrebbero subire variazioni sostanziali.

Per far questo è sicuramente utile e necessario fare riferimento oltre che, come è ovvio, a quanto stabilito dal Decreto, anche a quanto detto nella [Relazione illustrativa](#) che accompagna, come d'uso il Decreto (Esiste anche una Relazione Tecnica che però si limita a specificare come tutti gli articoli non comportino nuove spese ma che anzi in taluni casi comportano risparmi di spesa, anche se non sempre quantificabili a priori).

Non possiamo non ricordare che in qualche modo la riforma del CAD sembra partire in salita. Basta considerare che il Consiglio di Stato nel suo parere indica diversi punti critici, in particolare la mancata individuazione di tempi certi per la completa attuazione e per la effettiva implementazione del punto unico di accesso

a tutti i servizi della PA (il portale Italia Login), lo scarso coordinamento fra lo SPID e gli altri strumenti attraverso i quali i soggetti privati possono interloquire con la PA (Carta d'identità elettronica e Carta nazionale dei servizi), la mancata individuazione delle risorse. Qui purtroppo si sconta un problema irrisolto del modo di legiferare italiano; da una parte perché una norma possa passare è di fatto necessario che sia indicata come a costo zero, ed anche in questo caso la relazione tecnica si premura di spiegare, articolo per articolo come tutta la riforma sia senza nuovi oneri, dall'altra è evidente che una riforma che coinvolge numerosissimi soggetti e che richiede drastici cambiamenti nel modo di operare della PA difficilmente non avrà necessità di finanziamenti ad hoc.

Diverse critiche pure dalle Regioni<sup>64</sup>. Da più parti si sostiene pertanto in modo esplicito la necessità di interventi correttivi.<sup>65</sup>

### Modifiche riguardo alla PEC

Le modifiche apportate alla disciplina della PEC non sono per così dire “dirette”, nel senso che gli articoli del CAD che riguardano la trasmissione dei documenti per via telematica (art. 45 e 47) non vengono modificati in nulla mentre all'art. 48 sono aggiunti solo i rimandi a regole tecniche da emanare in base all'art. 71<sup>66</sup> (norme tecniche cui si fa riferimento in tutto l'articolato del D. Lgs e che saranno di nuovo “fondamentali” per completare il quadro normativo).

Va notato però che la riforma del CAD riguarda anche le disposizioni relative all'identità digitale dei cittadini e delle imprese, introduce il domicilio digitale della persona fisica e delle imprese e introduce lo SPID che dovrebbe diventare lo

---

<sup>64</sup> <https://www.key4biz.it/nuovo-cad-i-rilievi-delle-regioni-troppi-dettagli-tecnici/150231/>

<sup>65</sup> Il Consiglio di Stato afferma: “A fronte dell’importanza del progetto sotteso alla riforma del CAD, la Commissione speciale, quindi, non può esimersi dall’evidenziare alcuni fattori che potrebbero ‘compromettere’ il successo dell’iniziativa cui tende il decreto delegato e che, proprio per tale ragione, dovranno ora essere monitorati dall’Amministrazione e, ove necessario, divenire oggetto di adeguati interventi correttivi”

<sup>66</sup> Con l'art. 71 si introduce un unico decreto di regole tecniche di attuazione del CAD e questo rappresenta indubbiamente una semplificazione; tuttavia dato che viene anche cancellato il fatto che le regole tecniche pre-vigenti restano fino ad entrata in vigore delle nuove, questo significa che le nuove norme tecniche dovrebbero arrivare prima del 1 luglio 2016, data di entrata in vigore del Decreto. Tutto questo è certamente auspicabile, ma da molte parti si nutrono seri dubbi sulla possibilità che si riesca ad emanare le regole tecniche nei tempi previsti considerato che in passato sono stati necessari talvolta diversi anni per l’emanazione di provvedimenti similari a quelli previsti dall’art. 71. Va anche ricordato che fu proprio l’art. 71 ad introdurre la nozione di Regola tecnica e che ad oggi ne esistono qualche decina.

strumento privilegiato per accedere ai servizi della PA e per presentare istanze e dichiarazioni. Tutto questo avrà influenza notevole sul futuro della PEC. Cerchiamo di capire perché.

Anzitutto l'art. 3bis, ampiamente rimaneggiato, sancisce l'obbligo (anche se si parla di facoltà, dizione peraltro criticata dai molti che ritengono necessario uno switch off integrale in tempi rapidi per passare definitivamente dal cartaceo al digitale)<sup>67</sup> del domicilio digitale per il cittadino. Di fatto si tratta di obbligo poiché intanto *"Il domicilio di cui al comma 1 è inserito nell'Anagrafe nazionale della popolazione residente-ANPR e reso disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi"* ma soprattutto perché ***"Esso costituisce mezzo esclusivo di comunicazione da parte dei soggetti di cui all'articolo 2, comma 1"***<sup>68</sup>

Non solo, ma l'obbligatorietà è vieppiù sancita al successivo comma 3 bis, dove si dice : *"Agli iscritti all'ANPR che non abbiano provveduto a indicarne uno è messo a disposizione un domicilio digitale con modalità stabilite con decreto del Ministro dell'interno di concerto con il Ministro delegato per la semplificazione e la pubblica amministrazione, sentito il Garante per la protezione dei dati personali. Con lo stesso decreto sono individuate altre modalità con le quali, per superare il divario digitale, i documenti possono essere consegnati ai cittadini"*

Sembra dunque che da quanto esposto derivino almeno due conseguenze:

- i. in primis ai cittadini, che non dichiarino esplicitamente il proprio domicilio digitale esso dovrebbe essere assegnato dalla PA e anche se si rimanda ad un futuro decreto non si vede come possa trattarsi di qualcosa di molto diverso da una PEC o da qualcosa di molto simile (e qui occorre molta attenzione per non ripetere la esperienza, per molti versi fallimentare, della CEC PEC), magari diversamente denominata, visto che eIDAS parla genericamente di *"servizio elettronico di recapito certificato"*; d'altronde che questa sia la strada è confermato dal fatto che per professionisti e imprese il domicilio digitale, da inserire nella ANPR è l'indirizzo PEC già presente (e ricordiamolo,

---

67 "Al fine di facilitare la comunicazione tra pubbliche amministrazioni e cittadini, e' facolta' di ogni cittadino indicare al comune di residenza un proprio domicilio digitale"

68 Art. 3bis, comma 2

obbligatorio) in INI PEC (a meno che il professionista o l'impresa non decida diversamente).

Per capire un po' meglio quali siano le intenzioni dell'Esecutivo e le modalità con cui si intende dare pratica attuazione a quanto enunciato bisogna ricorrere alla relazione di accompagnamento al nuovo CAD dove si legge che “*L'invio di un documento digitale avverrà in due modi: direttamente nei confronti di chi avrà eletto un domicilio digitale oppure indirettamente nei confronti di chi non avrà il suddetto domicilio. In quest'ultimo caso lo Stato metterà a disposizione una “casella di posta virtuale” che verrà utilizzata dalle PA per inviare le comunicazioni ai destinatari. Trattandosi di “casella di posta virtuale”, l'erogatore del servizio stamperà, poi, il documento trasmesso in digitale e lo consegnerà al destinatario. Ciò consentirà a tutte le PA di produrre e trasmettere in digitale.*”

Ora il problema è che, anche se con la lodevole intenzione di limitare il *digital divide* e di estendere a tutti il domicilio digitale, si introduce in sostanza un altro tipo di PEC peraltro definita addirittura “virtuale” di cui non è ben chiaro ne chi pagherà i costi né in che modo praticamente essa sarà implementata. Sembra più che una soluzione al problema di quanti non comunicheranno volontariamente il loro domicilio digitale quasi un espediente per prendere tempo nell'attesa di trovare una soluzione più realistica. In ogni caso l'erogatore del servizio difficilmente lo farà a costo zero, considerato anche che la stampa e la spedizione in modalità “classica” costano assai di più di un invio telematico, senza considerare il problema della conformità all'originale e la necessità dell'apposizione del contrassegno elettronico sulla copia analogica.

- ii. l'altra conseguenza molto rilevante sta nell'uso della dicitura *mezzo esclusivo* riferito al domicilio digitale come modo di comunicazione da parte della PA e delle “*societa' a controllo pubblico, come definite nel decreto legislativo adottato in attuazione dell'articolo 18 della legge n. 124 del 201*” (sono gli altri soggetti di cui all'art.2 comma 1); questo significa che, stando almeno al significato letterale, anche nei rapporti con i cittadini, così come già stabilito

per imprese e professionisti, la carta dovrebbe sparire o addirittura essere considerata fuorilegge. Ora, se questo scenario costituisce in fondo l'applicazione radicale del principio “*digital first*” stabilito nella delega legislativa, la sua piena attuazione pone problemi non indifferenti soprattutto considerato che non esiste una norma esplicita che stabilisce cosa accade alle comunicazioni cartacee e costituisce una inversione completa di quanto oggi previsto, quantomeno in alcuni campi dato che se oggi arriva al cittadino una richiesta di pagamento tramite una mail essa non è valida, mentre da adesso in poi sarebbe la comunicazione cartacea ad essere invalida. Se poi si tiene conto che il CAD si applica anche al processo telematico, si capisce quanto complessa possa diventare la situazione. Probabilmente non resta da sperare che il regolamento di prossima attuazione chiarisca almeno in parte questi dubbi.

Un'altra questione che tocca da vicino la natura e la sorte futura della PEC sta nella introduzione dello SPID (Sistema Pubblico di identità digitale). Tramite SPID infatti le pubbliche amministrazioni potranno consentire l'accesso in rete ai vari servizi (relegando di fatto ad un ruolo marginale la carta d'identità elettronica e la carta nazionale dei servizi, anche se queste sembrerebbero in realtà presupposti per poter richiedere SPID). Tuttavia vengono introdotte alcune funzioni dello SPID che anche se formulate in modo poco chiaro (e secondo molti di difficile se non impossibile attuazione) sembrano presupporre un uso in qualche modo alternativo alla PEC o forse in coordinamento con questa. Infatti il comma 2 septies di nuova introduzione recita: “*Un atto giuridico può essere posto in essere da un soggetto identificato mediante SPID, nell'ambito di un sistema informatico avente i requisiti fissati nelle regole tecniche adottate ai sensi dell'articolo 71, attraverso processi idonei a garantire, in maniera manifesta e iniquivoca, l'acquisizione della sua volontà. Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa anche regolamentare in materia di processo telematico.*” Si tratta come si vede di una comma poco chiaro, che oltretutto rimanda di nuovo ad un futuro regolamento e fa salve le disposizioni riguardanti il processo telematico (e non è ben chiaro, considerato che tutto il processo telematico, nelle sue varie articolazioni è in

rapido movimento<sup>69</sup> perché sia stata introdotta una norma che di fatto impedisce l'applicazione integrale, senza se e senza ma del CAD anche ai vari tipi di processo telematico)

### **Modifiche riguardo alla Firma elettronica**

Nel nuovo CAD spariscono le definizioni di tutti i tipi di firma e rimane solo quella di firma digitale che viene ora definita come un particolare tipo di firma qualificata (in adesione a eIDAS). Infatti viene introdotto un articolo 1-bis che recita: *"Ai fini del presente Codice, valgono le definizioni di cui all'articolo 3 del regolamento (UE) 23 luglio 2014, n. 910, del Parlamento europeo e del Consiglio.."*.

Sembra poi di capire che in base all'art. 21<sup>70</sup> qualsiasi documento informatico, anche una semplice mail (in quanto di per sé stessa fornita di firma elettronica anche se non qualificata) soddisfi il requisito della forma scritta (il che andrebbe oltre quanto richiesto da eIDAS). Questa prospettiva viene giudicata piuttosto preoccupante perché non esisterebbe più una logica graduazione del valore giuridico e dell'efficacia probatoria del documento informatico in base alla firma elettronica che lo contraddistingue, ma un documento elettronico con una firma elettronica semplice potrebbe avere il valore giuridico e l'efficacia probatoria della scrittura privata. La questione peraltro è complicata dal fatto che si rimanda al solito emanando Regolamento, che richiederà magari, come già accaduto in passato anni. In ogni caso sembra difficile, in caso di contenzioso evitare la consulenza d'ufficio. E non sembra aggiungere certezze il fatto che comunque deve essere il Giudice a valutare, a posteriori, se nel caso concreto si tratti di firma elettronica conforme al Regolamento. Certo sarebbe vantaggioso per tutti e soprattutto eviterebbe contenziosi e spreco di tempo nell'amministrazione della giustizia l'avere certezze sulla validità a priori di documenti o firme. Si ripropone il solito dilemma sul rapporto tra normativa generale e Regolamenti

---

<sup>69</sup> Vedi il capitolo sull'uso di PEC e firma elettronica nel PT

<sup>70</sup> *"2. fermo restando quanto previsto dai commi 2-bis e 2-ter, il documento informatico sottoscritto con firma elettronica, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del codice civile. l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria".*

## **Modifiche riguardo alla Marca temporale**

Nel nuovo CAD si fa riferimento per la validazione temporale solo ed esclusivamente alle definizioni del Regolamento eIDAS. Infatti la parola "temporale" viene soppressa in tutto il corpo del provvedimento ogni volta che si trovava accanto al termine "validazione", mentre l'intera definizione della validazione temporale risulta soppressa (ex lett. bb) delle definizioni) Quando si parla all'art. 20, nuova formulazione, di "*Validità ed efficacia dei documenti informatici*", l'attributo "temporale" viene soppresso per cui si parla genericamente di validazione, sia quando ci si riferisce alle emanande Regole tecniche, che dovrebbero andare a sostituire quelle esistenti, sia quando ci si riferisce alla opponibilità a terzi di data certa di formazione. Dalla norma risultante non è davvero chiaro cosa sia la validazione di cui si parla. Infatti essa non è riportata come tale (ovvero nella sola dizione validazione) in eIDAS e quindi sembra qualcosa di diverso ma di assolutamente non chiaro.

D'altra parte il senso e l'argomento della norma sembrano chiari: stiamo parlando di validazione temporale e allora davvero non si capisce perché sopprimere l'attributo temporale.

## SENTENZE ESEMPLARI

### Introduzione

In questo capitolo si riportano e commentano alcune recenti sentenze sugli argomenti oggetto di studio. Non si vuole qui fare una rassegna esaustiva della giurisprudenza, ma riportare alcuni esempi particolarmente significativi. Si tratta di sentenze emanate da istanze giuridiche diverse (Tribunale, Commissione tributaria, Corte dei Conti, Cassazione) ad indicare l'importanza e la “pervasività” delle questioni qui trattate ed anche la mole di contenzioso che può nascere praticamente a tutti i livelli giuridici. Resta da capire se il contenzioso è il risultato della nota “litigiosità” italiana o se la grande complessità delle norme contribuisce a far nascere problemi di interpretazione ed attuazione delle norme stesse e pronunciamenti talvolta discordanti.

Sarebbe auspicabile, in questo come in tanti altri campi della legislazione, una profonda semplificazione, che limiti al massimo i motivi del contenzioso, anche tenendo conto dell'importanza economica che gli aspetti giuridici qui trattati posso avere (si pensi solo al problema della partecipazione ad appalti nazionali o internazionali). D'altra parte non sembra ancora il tempo di un “Testo unico” semplice e chiaro, proprio per la natura continuamente “in divenire” delle norme e soprattutto degli aspetti tecnici sottostanti alle norme stesse, senza considerare l'aspetto, in questo campo come in quasi tutti i campi legislativi, della valenza necessariamente “sovranazionale” di ogni normativa.

Le sentenze di seguito analizzate, appaiono di particolare interesse anche al fine di chiarire aspetti specifici degli strumenti elettronici qui esaminati che, come spesso accade in molti campi legislativi, sembrano risultare chiari nella loro formulazione (teorica) ma risultano poi complessi nella loro implementazione (pratica) e quindi le pronunce dei vari tribunali sono spesso utili a meglio determinare possibilità d'uso e caratteristiche specifiche dei vari strumenti o a specificarne la complessità laddove, come anche accade, neanche i tribunali sono in grado di districarsi in modo soddisfacente nel groviglio di norme.

## Caso 1 Il Consiglio di Stato

L'orientamento del Consiglio di Stato in materia di notifica via PEC ha destato diverse perplessità anche sulla base della analisi di alcune sentenze recenti.

In particolare con la sentenza 20 gennaio 2016, n. 189 la Terza Sezione del Consiglio di Stato nega la validità delle notificazioni a mezzo PEC nel processo amministrativo, argomentando ciò dalla specialità del rito (e conseguentemente negando validità alle disposizioni dettate in materia di processo civile telematico). L'unica possibilità di ritenere valida la notificazione a mezzo PEC si verificherebbe in presenza di un'autorizzazione preventiva da parte del Presidente, concessa ai sensi dell'art. 52 del Codice del Processo Amministrativo, insussistente nel caso di specie.

Questa sentenza è stata definita una “mazzata” giacché sembrava mettere una pietra tombale sulla possibilità dell'uso della PEC nel processo amministrativo e sembrava a molti, in qualche modo, troppo rigida e non giustificata anche rispetto alla normativa allora in vigore

Infatti, a prescindere dallo specifico procedimento, anzitutto sembra poco corretto non tenere conto che [la legge 21 gennaio 1994, n. 53](#) (Facoltà di notificazioni di atti civili, amministrativi e stragiudiziali per gli avvocati e procuratori legali) stabilisce in modo chiaro all'art 3 bis che: *La notificazione con modalità telematica si esegue a mezzo di posta elettronica certificata all'indirizzo risultante da pubblici elenchi, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici.*

Inoltre, e questo non può non causare qualche sconcerto, lo stesso Consiglio di Stato si era espresso, anche recentemente in senso opposto, in particolare con la sentenza della Sez. V, 22/10/2015, n. 4862 e addirittura con una sentenza proprio della Sezione Terza, la n. 4270 del 14 settembre 2015.

D'altra parte la sezione sesta, era intervenuta con la sentenza n. 2682 del 28 maggio 2015 e si era pronunciata in senso positivo rispetto alla validità della notifica a mezzo PEC stabilendo che “*la mancata autorizzazione presidenziale ex art. 52, c o. 2, del c.p.a. non può considerarsi ostativa alla validità ed efficacia*

*della notificazione del ricorso a mezzo PEC atteso che nel processo amministrativo trova applicazione immediata la l. n. 53 del 1994 (ed in particolare... gli articoli 1 e 3 bis della legge stessa), nel testo modificato dall'art. 25 co. 3, lett. a) della l. 12 novembre 2011, n. 183, secondo cui l'avvocato "può eseguire la notificazione di atti in materia civile, amministrativa e stragiudiziale... a mezzo della posta elettronica certificata.*

L'intervento della sezione sesta era avvenuto proprio per cercare di mettere ordine in una materia in cui ogni TAR sembrava andare “per conto suo”, dato che, da una parte, il TAR Lazio-Roma Sez. III n. 11808/14, il TAR Calabria Sez. II n. 183/15, il TAR Campania-Napoli Sez. VI n. 923/15 hanno ritenuto pienamente valide ed efficaci, nel processo amministrativo, le notifiche degli avvocati tramite PEC ma, dall'altra il TAR Lazio-Roma Sez. II ter n. 396/15, TAR Veneto Sez. III n. 369/15, TAR Abruzzo-Pescara Sez. I n. 49/15, hanno al contrario affermato la non applicabilità delle stesse.

Nonostante il pronunciamento, prima della sesta e poi della terza sezione sia molto chiaro, il TAR Campania Sez.VI è tornato sulla questione negando l'utilizzabilità della PEC come mezzo di notifica.

Una situazione quindi complessa e non priva di confusione.

La novità sta nella emanazione del decreto del Presidente del Consiglio dei Ministri n. 40 del 16 febbraio 2016 che fissa le regole tecnico-operative per l'attuazione del processo amministrativo telematico, introdotto a partire dal 1° luglio 2016. Senza entrare nei dettagli del provvedimento basterà dire, per quanto riguarda i problemi qui analizzati che il provvedimento definisce il sistema informativo della giustizia amministrativa (SIGA) l'insieme delle risorse hardware e software, mediante le quali la giustizia amministrativa tratta in via automatizzata attività, dati, servizi, comunicazioni e procedure relative allo svolgimento dell'attività processuale e stabilisce che il SIGA gestisce con modalità informatiche in ogni grado del giudizio la formazione del fascicolo e tutte le operazioni connesse al processo amministrativo telematico. Inoltre si stabilisce che le comunicazioni avvengono tramite PEC e l'art. 14 delle specifiche tecniche dispone che "*Le notificazioni da parte dei difensori possono essere effettuate*

*esclusivamente utilizzando l'indirizzo PEC risultante dai pubblici elenchi, nei confronti dei destinatari il cui indirizzo PEC risulti dai medesimi pubblici elenchi. Le notificazioni nei confronti delle pubbliche amministrazioni non costituite in giudizio sono effettuate esclusivamente avvalendosi degli indirizzi PEC del Registro delle P.P. AA., fermo restando quanto previsto, anche in ordine alla domiciliazione delle stesse, dal regio decreto 30 ottobre 1933, n. 1611, in materia di rappresentanza e difesa in giudizio dello Stato".*

Questo dovrebbe impedire per il futuro il ripetersi di decisioni contraddittorie in materia di notifica telematica da parte di TAR e Consiglio di Stato, dato che anche se da più parti si auspicava un maggiore coraggio nella innovazione<sup>71</sup>, la notifica telematica diventa obbligatoria.

Resta tuttavia il fatto che ci sono stati pronunciamenti decisamente diversi sulla stessa questione e questo indica di nuovo che, almeno sino ad ora, la normativa poteva produrre interpretazioni contrastanti.

## Caso 2 La firma digitale nel giudizio della Cassazione

Si analizza qui una recente sentenza della Corte di Cassazione che a prescindere dal suo significato tecnico è utile per valutare l'orientamento della Suprema Corte in materia considerando anche le motivazioni e le norme su cui queste sono fondate

La Corte di Cassazione con la sentenza n. 22871/2015 del 10/11/2015 ha affrontato per la prima volta le questioni afferenti la firma digitale e specificamente se la sentenza firmata digitalmente debba ritenersi inesistente in quanto priva della sottoscrizione autografa ex art. 132, n. 5, c.p.c. La Suprema Corte ha attribuito correttamente piena rilevanza giuridica alla firma digitale della sentenza fondando la motivazione su un complesso di norme tra cui il CAD (D.Lgs. 82/2005), le regole e le specifiche tecniche del PCT.

Ciò che qui va messo in evidenza è un insieme di principi cui la corte fa riferimento e le conseguenze che ne trae.

---

<sup>71</sup><http://www.diritto24.ilsole24ore.com/art/dirittoAmministrativo>

Anzitutto facendo riferimento anche a sentenze precedenti della stessa Cassazione la Suprema Corte definisce in modo univoco la firma apposta per sottoscrizione ovvero “*un segno grafico che abbia caratteristiche di specificità sufficienti e possa quindi svolgere funzioni identitarie e di riferibilità soggettiva, pur nella sua eventuale illeggibilità (la quale non inficia la idoneità della sottoscrizione se sussistono adeguati elementi per il collegamento del segno grafico con un'indicazione nominativa contenuta nell'atto)*” Quindi si evidenzia la funzione che nel caso di sottoscrizione di sentenza la firma svolge ovvero funzione identitarie e di riferibilità soggettiva.

Poi viene confermata la applicabilità del CAD al processo civile telematico in quanto ”... l’art. 4 del decreto legge n. 193 del 2009, convertito nella legge n. 24 del 2010, intitolato «misure urgenti per la digitalizzazione della giustizia» ha esteso al processo civile i principi previsti dal decreto legislativo 7 marzo 2005 n. 82 e successive modificazioni (codice dell’amministrazione digitale) ... ”.

La Corte precisa ulteriormente che ”*Quindi i principi generali del C.A.D. sono applicabili anche in ambito processuale e le relative disposizioni costituiscono le norme con valore di legge ordinaria che, per il tramite dell’art. 4 del d.l. n. 193 del 29 dicembre 2009, convertito nella legge n. 24 del 22 febbraio 2010, disciplinano gli atti del processo civile redatti in forma di documento informatico (cfr. art. 1 lett. p e art. 20 C.A.D.) e sottoscritti con firma digitale (cfr. art. 1 lett. s e art. 21 C.A.D.)*”.

Infine considerando anche che solo tramite la firma elettronica è possibile il deposito della sentenza nel fascicolo telematico la Corte conclude affermando un chiaro principio di diritto ”*va perciò affermato che la sentenza redatta in formato elettronico dal giudice e da questi sottoscritta con firma digitale ai sensi dell’art. 15 del D.M. 21 febbraio 2011 n. 44, non è affetta da nullità per mancanza di sottoscrizione, sia perché sono garantite l’identificabilità dell’autore, l’integrità del documento e l’immodificabilità del provvedimento (se non dal suo autore), sia perché la firma digitale è equiparata, quanto agli effetti, alla sottoscrizione autografa in forza dei principi contenuti nel decreto legislativo 7 marzo 2005 n.*

*82 e succ. mod., applicabili anche al processo civile, per quanto disposto dall'art. 4 del d.l. 29 dicembre 2009 n. 193, convertito nella legge 22 febbraio 2010 n. 24".*

Si tratta come si può vedere di un principio in qualche modo ovvio soprattutto alla luce dell'introduzione e dello sviluppo del processo telematico a tutti i livelli ma risulta interessante la logica seguita nelle argomentazioni e la chiarezza del principio formulato.

### **Caso 3 Inesistente la notifica tramite pec senza la ricevuta di avvenuta consegna.**

La sentenza n. 20072/2015 qui analizzata è stata emessa dalla Sezione Lavoro della Cassazione il 19 maggio 2015.

Il motivo di interesse sta qui nel fatto che La Cassazione entra in merito alla struttura per così dire “concettuale della PEC”, richiamando più volte l’analogia con la notifica cartacea ed evidenziando come fatti che possono apparire meramente “tecnici” possono avere conseguenze sostanziali sul valore della notifica Infatti i Giudici evidenziano che la notifica a mezzo posta elettronica certificata non si esaurisce con l’invio telematico dell’atto, ma si perfeziona con la consegna del plico informatico nella casella di posta elettronica del destinatario, e la prova di tale consegna è costituita dalla ricevuta di avvenuta consegna.

Si fa riferimento alla L. n. 53 del 1994 e succ. mod., in particolare evidenziando che il comma 3 dell’art. 3 bis della suddetta L. n. 53, introdotto dalla L. n. 228 del 2012, prevede che la notifica effettuata con modalità telematica si perfeziona, per il soggetto notificante, nel momento in cui viene generata la ricevuta di accettazione prevista dall’articolo 6, comma 1, del D.P.R. 11 febbraio 2005, n. 68, e, per il destinatario, nel momento in cui viene generata la ricevuta di avvenuta consegna prevista dall’articolo 6, comma 2, dello stesso D.P.R.

Dalla mancanza della ricevuta di consegna (e di quella di accettazione) consegue che il processo notificatorio non è concluso. Pertanto, afferma la Corte, “*la mancata produzione della ricevuta di avvenuta consegna della notifica a mezzo p.e.c. del ricorso per cassazione, impedendo di ritenere perfezionato il procedimento notificatorio, determina quindi l’inesistenza della notificazione, con conseguente impossibilità per il giudice di disporne il rinnovo ai sensi dell’art.*

*291 cod. proc. civ., in quanto la sanatoria ivi prevista è consentita nella sola ipotesi di notificazione esistente, sebbene affetta da nullità.*" La sentenza è particolarmente interessante perché connessa ai problemi di conservazione dei documenti elettronici prodotti nei vari passaggi tramite cui l'invio della PEC si concretizza.

#### **Caso 4 Il destinatario dell'atto non può eccepire di non aver letto il messaggio o di non averlo ricevuto per difficoltà tecniche o malfunzionamenti della rete telefonica o telematica**

Si tratta di una sentenza ( n. 9892/2015 della Corte di Cassazione Penale ) che riprende una giurisprudenza ormai consolidata. Il suo interesse sta nel fatto che specifica in modo non univoco cosa debba intendersi per notifica e quando la notifica a mezzo PEC può considerarsi compiuta.

Un avvocato aveva fatto ricorso lamentando la mancata lettura di una notifica ricevuta via posta elettronica certificata, a causa di un guasto informatico.

Il ricorso è stato respinto.

I giudici infatti argomentano anzitutto l'idoneità della PEC quale mezzo di notifica anche nel processo penale facendo derivare questa affermazione dal d.l. 29 dicembre 2009, n. 193 recante "*Interventi urgenti in materia di funzionalità del sistema giudiziario*", il quale, all'art. 4, comma 2, ha previsto che nel processo civile e nel processo penale, secondo le regole tecniche che verranno previste da successivi decreti, le comunicazioni e le notificazioni sono effettuate mediante PEC nei confronti di soggetti diversi dall'imputato e dal successivo art. 16 del d.l. 18 ottobre 2012, n. 179 secondo il quale, per le notifiche a persona diversa dall'imputato a mezzo PEC, "*la relazione di notificazione è redatta in forma automatica dai sistemi informatici in dotazione alla cancelleria*".

Ribadita quindi l'idoneità della PEC quale mezzo di notifica, i Giudici facendo prima riferimento all'art. 48 del d.lgs. 7 marzo 2005 n. 82 (Codice dell'amministrazione digitale) il quale prevede che "*La trasmissione del documento informatico per via telematica, equivale, salvo che la legge disponga*

*diversamente, alla notificazione per mezzo della posta. La data e l'ora di trasmissione e di ricezione di un documento informatico sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche” e poi al d.P.R. 11 febbraio 2005, n. 68; in particolare, all’art. 4 che prevede la validità agli effetti di legge della posta elettronica certificata e, soprattutto, all’art. 3 che sancisce che “il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all’indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore” i giudici ribadiscono che la notifica si dà per consegnata quando in base al successivo art. 6 del citato d.P.R., “il gestore di posta elettronica certificata utilizzato dal mittente fornisce al mittente stesso la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione di un messaggio di posta elettronica certificata”.*

Per questi motivi ed anche in analogia con quanto stabilito dalla stessa Corte in merito ai messaggi non letti della segreteria telefonica, la Corte stabilisce che la notifica dell'avviso dell'udienza deve ritenersi ritualmente effettuata e respinge il ricorso.

#### **Caso 5 PEC valida anche senza firma elettronica**

Con la [sentenza n. 1450, depositata il 10 marzo del 2015](#), il Tribunale Amministrativo Regionale (TAR) della Campania ha accolto un ricorso del Comune di Terzigno che aveva presentato quattro istanze alla Regione Campania, inviandole in allegato a un messaggio di posta elettronica certificata senza firmarle digitalmente, e si era visto rifiutare le domande proprio per la mancanza della sottoscrizione digitale.

La sentenza in oggetto risulta particolarmente interessante in quanto ha generato opinioni discordi tra quanti l'hanno analizzata.

Nell'[approfondimento di Sarah Ungaro e Stefano Frontini per il sito di ANORC](#)<sup>72</sup> (Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale) si esprime un profondo disaccordo con la sentenza (vedremo tra un attimo i motivi di questo disaccordo) mentre opposta è l'opinione di **Francesco Giuda** (espressa sulle pagine del [sito Altalex](#))<sup>73</sup> che si dichiara pienamente d'accordo con la decisione dei giudici amministrativi campani.

Cerchiamo sommariamente di capire come una questione apparentemente piuttosto chiara possa dar luogo a orientamenti così diversi.

La questione di fondo riguarda l'art. 65 del Codice dell'Amministrazione digitale (D.Lgs. n. 82/2005) che alla lettera. c-bis), disciplina la cosiddetta Pec-ID stabilendo che "*le istanze e le dichiarazioni presentate per via telematica alle P.A. e ai gestori di servizi pubblici ai sensi dell'art 38, commi 1 e 3, del decreto DPR 455/2000 sono valide se trasmesse dall'autore mediante propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'art. 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato*"<sup>74</sup>.

La norma sopra riportata riguarda la Pec Id ovvero una PEC rilasciata sulla base di strumenti di identificazione del titolare più stringenti rispetto a quelli usati nella PEC "ordinaria", fatto attestato dal gestore del sistema nel messaggio o in suo allegato. Ciò è chiaro se si considera il DPCM 27 settembre 2012 - *regole per identificare il titolare PEC* emanato proprio per dare attuazione a quanto stabilito dall'art. 65 lettera c-bis del CAD. Poiché, argomentano Ungaro e Frontini, non vi è evidenza che quella usata dal comune di Terzigno fosse una PEC Id la sentenza è frutto di un fraintendimento del Giudice e non interpreta correttamente la normativa.

Diversamente argomenta Francesco Giuda che nell'articolo citato non ritiene che la PEC da cui inviare un documento privo di firma elettronica alla PA debba essere necessariamente una PEC-Id perché l'invio sia da considerarsi valido.

<sup>72</sup>[http://www.anorc.it/notizia/656\\_Pec\\_o\\_Pec-ID\\_la\\_confusione\\_del\\_TAR\\_CAMPANIA](http://www.anorc.it/notizia/656_Pec_o_Pec-ID_la_confusione_del_TAR_CAMPANIA)

<sup>73</sup><http://www.altalex.com/documents/news/2015/03/31/istanza-all-a-pa-via-pec>

<sup>74</sup> Il comma rimane invariato anche dopo le modifiche apportate al CAD

Evidenzia pure il riferimento all'art 61 del D.P.C.M. 22 febbraio 2013, recante “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali” che stabilisce che “*L'invio tramite posta elettronica certificata di cui all'art. 65, comma 1, lettera c-bis) del Codice, effettuato richiedendo la ricevuta completa di cui all'art. 1, comma 1, lettera i) del decreto 2 novembre 2005, recante “Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata” sostituisce, nei confronti della pubblica amministrazione, la firma elettronica*”.

Posizioni diverse come si vede e anche se chi scrive propende (da un punto di vista strettamente formale) più per la prima posizione, non si può che ribadire la difficoltà di orientarsi in questo tipo di normativa. Va anche sottolineato che, se il riferimento alla PEC-Id rimane anche dopo le modifiche che apporterà lo SCHEMA DL 20/01/2016, esso perde tuttavia di significato alla luce di eIDAS.

Nella direzione della validità della trasmissione via PEC di istanze alla PA da parte dei cittadini si era già espresso il Consiglio di Stato con l'Ordinanza del 15 gennaio 2015 riguardante la sentenza del TAR Puglia 6 agosto 2014, n. 011030, con la quale, il Tribunale Amministrativo Regionale si era pronunciato in merito a una questione riguardante un'istanza inviata tramite CEC-PAC, ma considerata irricevibile dalla Regione Puglia in quanto priva di sottoscrizione, ribadendo non solo la validità della trasmissione ma anche l'irrilevanza della mancanza di sottoscrizione dei documenti allegati, ma va notato che nel caso specifico si trattava di CEC PAC, un tipo di PEC (peraltro ormai dismessa) che richiedeva una identificazione “forte” dell'intestatario e quindi in qualche modo potrebbe essere assimilata ad una PEC ID.

Va rilevato che in questo ultimo caso, come in quello della sentenza del TAR Campania citata in questo stesso paragrafo, la mancata sottoscrizione riguarda un allegato al messaggio di posta e rimane ancora prevalente tra i giuristi l'opinione che il messaggio e l'eventuale allegato sono documenti informatici distinti e se l'allegato non è sottoscritto, il fatto che sia allegato ad un messaggio PEC di cui è

certa la provenienza, non lo rende, *ipso facto*; riconducibile con certezza all'intestatario della PEC stessa.<sup>75</sup>

### Caso 6 Notifica con PEC inutile se l'azienda non ha la firma digitale

Il motivo di interesse di questa sentenza sta nel fatto che come argomenta Rossella Ragosta nella analisi riportata sul sito [www.agendadigitale.eu](http://www.agendadigitale.eu)<sup>76</sup> essa sembra andare in decisa controtendenza rispetto agli orientamenti giuridici prevalenti.

La sentenza del Tribunale di Lecce del 16 marzo del 2016 dispone in sostanza che la: “Notifica con PEC è inutile se l'azienda non ha la firma digitale”.

Il problema nasce dal fatto che alla richiesta di rinnovo della notifica nei confronti della società resistente il Giudice valutato il mancato ricevimento del ricorso aveva ordinato il “*rinnovo della rinotifica secondo l'ordinario procedimento a mezzo ufficiale giudiziario*”, in quanto dal dispositivo di sentenza il Giudice ha così ritenuto: “*la normativa che impone alle imprese di dotarsi di casella di posta elettronica certificata non le obbliga a munirsi di un programma elettronico che consente l'apertura degli atti firmati digitalmente*”.

La decisione appare sconcertante in quanto è dato ormai per acquisito che la PEC ha certamente lo stesso valore legale di una raccomandata con ricevuta di ritorno, come peraltro stabilisce la normativa vigente; per il soggetto notificante la notifica si perfeziona nel momento in cui viene generata la ricevuta di accettazione e per il destinatario, nel momento in cui viene generata la ricevuta di avvenuta consegna (entrambe le ricevute sono previste dal DPR 11/2005 n. 68).

Peraltro neanche la mancanza dell'avviso di ricevimento inficia la validità di una raccomandata, come conferma la decisione adottata dalla Cassazione Civile Sez. III con sentenza n. 16327 pubblicata il 24/07/2007, in quanto ha ritenuto che” *la lettera di raccomandata – anche in mancanza dell'avviso di ricevimento costituisce prova certa della spedizione attestata dall'ufficiale postale attraverso*

---

<sup>75</sup> Vedi ad es. <http://www.forumpa.it/pa-digitale/ancora-poca-chiarezza->

<sup>76</sup> <http://www.agendadigitale.eu/egov/notifica-con-pec-inutile>

*la ricevuta..*”, da cui consegue che per la PEC già la sola ricevuta di accettazione può costituire prova dell'avvenuta notifica.

Qui in realtà non si tratta di nulla che riguardi la PEC ma il fatto che chi la riceve, non avendo, a detta del Giudice l'obbligo di dotarsi di un *programma elettronico che consente l'apertura degli atti firmati digitalmente* può rifiutare qualsiasi notifica tramite PEC che contenga documenti firmati digitalmente il che risulta quanto meno paradossale dato che le notifiche via PEC contengono di norma documenti firmati digitalmente (ricordiamo che la PEC è, di fatto, un mero contenitore). Se la tesi sostenuta in questa sentenza avesse una qualche validità sarebbe sostanzialmente impossibile il Processo Telematico. Va anche detto che è ormai invalso l'uso (reso addirittura obbligatorio dalle recenti norme sul processo amministrativo telematico)<sup>77</sup> di una forma di firma elettronica (la PADES) che non necessita di programmi particolari per aprire i documenti firmati digitalmente. Sembra pertanto che la sentenza in esame sia risultato di una non perfetta comprensione dei meccanismi della PEC e della firma elettronica.

### **Considerazioni sulle sentenze analizzate**

Si sono riportate e parzialmente analizzate alcune sentenze molto recenti sugli argomenti oggetto di analisi da cui si ricava che, anche se si stanno consolidando orientamenti condivisi nella relativa giurisprudenza (orientamenti che dovrebbero essere favoriti nella loro uniformità da alcune normative recenti che tendono a semplificare e rendere omogenee le diverse procedure di firma e notifica elettronica), permane ancora tra i giudici una sorta di incertezza di fondo ed un legame ancora troppo forte con le corrispettive procedure analogiche (che senso ha ad esempio scrivere “*firme apposta in calce al documento informatico*”<sup>78</sup>) le quali portano a pronunciamenti che non sempre sembrano in linea con la lettera e lo spirito della normativa vigente (come nel caso della sentenza del Tribunale di Lecce del 16 marzo del 2016).

---

<sup>77</sup> DPCM 16 febbraio 2016 n. 40 contenente le regole e specifiche tecniche per l'attuazione del processo amministrativo telematico

<sup>78</sup> Accade nella pronuncia n. 22871 del 10 novembre 2015 della Corte di Cassazione che recita: “*la firma digitale, quando si trova in calce alla sentenza....*”

## CONCLUSIONI

La normativa italiana sugli strumenti digitali che permettono di procedere verso l'informatizzazione di molti procedimenti, in particolare nella PA, con i prevedibili vantaggi in termini di risparmio di tempo e di risorse e di semplificazione delle procedure, presenta luci e ombre.

Da una parte una adozione precoce, rispetto ad altri paesi europei, di questi strumenti, ha permesso di accumulare un notevole bagaglio di esperienza in questo campo, sia dal punto di vista tecnico che da quello commerciale.

Dall'altra, l'eccesso di normative, sovrapposte e modificate ripetutamente nel tempo porta a pensare che solo interventi molto radicali e mirati possono semplificare una situazione che appare per molti versi piuttosto ingarbugliata e non sempre facile da armonizzare con le disposizioni europee.

L'analisi della giurisprudenza, e di alcune sentenze in particolare, permette di affermare che il contenzioso nato attorno agli strumenti informatici qui presi in esame risulta decisamente elevato ed è con tutta probabilità il frutto di un eccesso di normative e del fatto che si fatica ad usare, come imporrebbe la questione, un paradigma completamente nuovo, continuando ad applicare analogie col mondo cartaceo e analogico che, soprattutto alla luce degli sviluppi tecnologici, non ha più molto senso.

Il cambiamento continuo, non sempre dovuto alla inadeguatezza degli organismi politici e tecnici che scrivono e mettono in pratica le regole in questo campo, produce ambiguità e incertezze che molto spesso neanche le perizie tecniche sono in grado di dissipare.

Sarebbe auspicabile rimarcare, anche nelle normative, la neutralità tecnologica degli strumenti informatici e anche se questo non eliminerebbe la necessità di perizie tecniche, almeno non costringerebbe il giudice a sentirsi ingabbiato in specifiche tecniche troppo stringenti da diventare obsolete in poco tempo e quindi non facilmente applicabili, così come sarebbe necessario non introdurre sempre nuovi tipi di strumenti (ad oggi non è chiaro praticamente a nessuno quanti e quali

tipi di PEC esistono e quali siano poi quelli immediatamente e praticamente applicabili nei vari contesti).

Sarebbe altresì auspicabile limitare al massimo l'adozione di provvedimenti presi dalle singole istanze della PA (circolari ed altro) che magari sono utili all'utente che spesso non saprebbe districarsi tra normative complesse e all'operatore che riceve indicazioni più chiare su cosa praticamente fare in molte situazioni che le norme di carattere generale non possono prevedere nel dettaglio, ma che se scritte senza la dovuta attenzione a non interferire o entrare in conflitto con la normativa di grado superiore possono a loro volta generare incertezza e contenzioso.

Infine se va certamente rimarcata la specificità della PA, che richiede spesso interventi *ad hoc* (si pensi alla specificità dei procedimenti giudiziari nelle loro diverse articolazioni o delle procedure degli appalti pubblici), probabilmente l'adozione degli strumenti informatici è una di quelle cose che possono spingere ad una maggiore uniformità nelle procedure nel campo pubblico e in quello privatistico col vantaggio evidente di chiarezza, trasparenza e facilità di gestione.

Le disposizioni più recenti sembrano andare, almeno in parte nella direzione qui auspicata, anche se da più parti si invoca un maggiore coraggio ed una maggiore radicalità nel cambiamento. La creazione di piattaforme analoghe a quelle implementate per portare avanti i vari tipi di processo telematico (PTT-SIGIT, SIGA) che presentano una certa rigidità ma permettono di ridurre al massimo errori e contenzioso, dato che prevedono la compilazione di moduli standard e l'invio delle comunicazioni in modi automatizzati e ben determinati e quindi difficilmente oppugnabili, sembrano una buona risposta a diversi dei problemi qui posti.

D'altra parte le novità che l'informatica introduce in tutti i campi sono tali che risulta per gli operatori, soprattutto se non più giovanissimi, molto difficile adeguarsi e abituarsi ai nuovi modi di pensare e quindi è prevedibile ancora per un tempo presumibilmente abbastanza lungo il protrarsi del periodo di apprendistato che, volenti o nolenti, tutti coloro che hanno a che fare con le nuove tecnologie e non sono, come si dice, *nativi digitali*, devono superare.

## **ABBREVIAZIONI**

Si riportano nell'elenco che segue solo le abbreviazioni specifiche usate in questo lavoro. Per le abbreviazioni di carattere generale, allo scopo di non appesantire la trattazione si rimanda ai siti che specificano le modalità di compilazione della tesi e forniscono elenchi di abbreviazioni standard<sup>79</sup>

- AgID Agenzia per l'Italia Digitale  
ANPR Anagrafe Nazionale della Popolazione Residenti  
CAD Codice dell'Amministrazione Digitale  
CADES CMS Advanced Electronic Signature  
CNIPA Centro nazionale per l'informatica nella pubblica amministrazione  
DigitPA Ente nazionale per la digitalizzazione della Pubblica amministrazione  
eIDAS electronic IDentification Authentication and Signature  
FE firma elettronica FD firma digitale FA firma avanzata FQ firma qualificata  
INI-PEC Indice Nazionale degli Indirizzi di Posta Elettronica Certificata  
IPA Indice delle Pubbliche Amministrazioni  
MT marca temporale  
PA Pubblica Amministrazione  
PADES PDF Advanced Electronic Signature
- PTT processo Tributario Telematico  
PEC posta elettronica certificata  
RED Registered Electronic Delivery  
ReGlndE Registro Indirizzi Elettronici  
SCHEMA DL 20/01/2016 SCHEMA DI DECRETO LEGISLATIVO RECANTE MODIFICHE E INTEGRAZIONI AL CODICE DELL'AMMINISTRAZIONE DIGITALE DI CUI AL DL 7 MARZO 2005, N. 82, AI SENSI DELL'ART. 1 DELLA LEGGE 7 AGOSTO 2015, N. 124  
SIGA Sistema Informativo della Giustizia Amministrativa  
SIGIT Sistema Informativo della Giustizia Tributaria  
SPID Sistema Pubblico per la gestione dell'Identità Digitale  
XADES XLM Advanced Electronic Signature

---

<sup>79</sup> In particolare vedi il corso di Tecniche di redazione per le dissertazioni di laurea <http://virtualcampus.unimarconi.it/>

## BIBLIOGRAFIA

Considerato il tipo di analisi effettuata in questo lavoro, riguardante norme e sentenze recentissime si è fatto riferimento essenzialmente a riviste e articoli on line (tutti visitati e verificati il 29 aprile 2016). Infatti lo sviluppo rapidissimo delle tecnologie e la relativa “rincorsa” del legislatore, oltre a quella che qualcuno chiama “*normatite acuta*”<sup>80</sup> e la necessità di adeguamento alla normativa comunitaria (e pure l’Europa non scherza in quanto a “*normatite*”), rendono obsolete in pochi anni, o addirittura mesi, ogni pubblicazione a stampa che cerchi di porsi come un compendio della materia. Per questo le riviste on line, alcune delle quali hanno ormai tradizione e prestigio consolidati, rimangono il riferimento principe per ogni discorso sugli argomenti trattati in questo lavoro. Solo per la parte di carattere più generale si è fatto riferimento ad alcuni testi “classici” dell’informatica giuridica, essenzialmente a:

G. Peruginelli, M. Ragona (a cura di) L’Informatica Giuridica in Italia, 2014, ESI

Nella versione digitale di questo lavoro i titoli e numeri delle norme e delle sentenze sono essi stessi collegamenti ipertestuali ai siti dove i documenti possono essere reperiti. Nella versione a stampa i collegamenti sono evidenziati dal colore e dal carattere sottolineato. Si è preferito riportare in nota il collegamento ipertestuale, in forma abbreviata ma funzionante, per rendere più agevole la lettura del testo. Si è ritenuto opportuno non inserire in questo elenco i rimandi alla normativa e alle sentenze, presenti nel corpo del testo. Di seguito l’elenco completo dei riferimenti.

<https://archiviando.wordpress.com/2015/02/23/la-pec-un-prodotto-made-in-italy/>

<http://digitalia.sbn.it/article/view/440>

[https://docs.google.com/document/d/16f\\_dP-PJhWEeALdCEcn8ZRKbKSnudOrxZlFBMcQRZyI/edit?ts=56b9da98](https://docs.google.com/document/d/16f_dP-PJhWEeALdCEcn8ZRKbKSnudOrxZlFBMcQRZyI/edit?ts=56b9da98)

<http://espresso.repubblica.it/opinioni/legge-e-liberta/2015/07/29/news/quello-strapotere-chiamato-legge-delega-1.223105>

<http://futuropdigitale.infocert.it/nuovo-ape-e-firma-digitale-per-scrivere-il-futuro-della-certificazione-energetica/>

[http://pst.giustizia.it/PST/it/pst\\_2\\_4.wp](http://pst.giustizia.it/PST/it/pst_2_4.wp)

---

<sup>80</sup>Parlano di questa strana malattia, in senso ironico, ovviamente, Luca Attias e Michele Melchionda della Corte dei Conti in un articolo, seguito da commenti interessanti, qui reperibile <http://www.forumpa.it/riforma-pa/la-tecnologia-non-la-si-interpreta-la-si-fa-per-una-de-normazione-sul-digitale>

<http://sportelloconsumatori.org/blog/2014/12/20/muore-la-posta-certificata-statale-fine-di-uno-spreco/>

[http://www.agendadigitale.eu/egov/cad-ripensare-la-riforma-pa-ecco-tutti-i-punti-critici\\_2133.htm](http://www.agendadigitale.eu/egov/cad-ripensare-la-riforma-pa-ecco-tutti-i-punti-critici_2133.htm)

[http://www.agendadigitale.eu/egov/notifica-con-pec-inutile-se-l-azienda-non-ha-la-firma-digitale\\_2099.htm](http://www.agendadigitale.eu/egov/notifica-con-pec-inutile-se-l-azienda-non-ha-la-firma-digitale_2099.htm)

[http://www.agendadigitale.eu/identita-digitale/che-restera-del-cad-dopo-la-riforma-ecco-tutte-le-modifiche-necessarie\\_1885.htm](http://www.agendadigitale.eu/identita-digitale/che-restera-del-cad-dopo-la-riforma-ecco-tutte-le-modifiche-necessarie_1885.htm)

<http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche/avvisi>

<http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/conservazione>

<http://www.agid.gov.it/node/2251>

<http://www.altalex.com/documents/news/2012/10/10/art-2215bis-c-c-la-marcatura-temporale-e-la-marca-temporiale>

<http://www.altalex.com/documents/news/2015/03/31/istanza-all-a-pa-via-pec-ma-priva-di-firma-digitale-e-improcedibile>

[http://www.anorc.it/notizia/253\\_Il\\_glifo\\_protegge\\_solo\\_se\\_stesso.html](http://www.anorc.it/notizia/253_Il_glifo_protegge_solo_se_stesso.html)

[http://www.anorc.it/notizia/656\\_Pec\\_o\\_Pec-ID\\_la\\_confusione\\_del\\_TAR\\_CAMPANIA\\_sulle\\_modalit\\_di\\_comunicazion.html%C3%B9](http://www.anorc.it/notizia/656_Pec_o_Pec-ID_la_confusione_del_TAR_CAMPANIA_sulle_modalit_di_comunicazion.html%C3%B9)

<http://www.cittadininternet.it/2013/04/07/pec-incompatibile-lo-dice-iscom-il-mediatore-europeo-si-scusa-con-cittadini-di-internet/>

[http://www.cortecostituzionale.it/documenti/convegni\\_seminari/STU%20210\\_DELEGA\\_LEGISLATIVA.pdf](http://www.cortecostituzionale.it/documenti/convegni_seminari/STU%20210_DELEGA_LEGISLATIVA.pdf)

<http://www.dirittodisapere.it/2015/09/03/pec-comunicare-con-la-pubblica-amministrazione-costa/>

[http://www.diritto24.ilsole24ore.com/art/dirittoAmministrativo/2016-03-24/al-via-processo-amministrativo-telematico-pubblicate-regole-tecnico-operative-122442.php?refresh\\_ce=1](http://www.diritto24.ilsole24ore.com/art/dirittoAmministrativo/2016-03-24/al-via-processo-amministrativo-telematico-pubblicate-regole-tecnico-operative-122442.php?refresh_ce=1)

<http://www.e-idas.org/eidas-regolamento-articolo-2/>

<http://www.forumpa.it/pa-digitale/ancora-poca-chiarezza-sulla-verifica-di-sottoscrizione-e-provenienza-delle-istanze-telematiche-allpa>

<http://www.forumpa.it/pa-digitale/caccia-ma-se-il-cad-non-si-adegua-a-eidas-rischialabrogazione>

<http://www.forumpa.it/pa-digitale/documenti-il-futuro-europeo-della-pec-necessarie-nuove-regole-tecniche>

<http://www.forumpa.it/pa-digitale/il-cad-che-ho letto-e-il-cad-che-sognavo>

<http://www.forumpa.it/pa-digitale/ancora-poca-chiarezza-sulla-verifica-di-sottoscrizione-e-provenienza-delle-istanze-telematiche-allpa>

<http://www.ilfattoquotidiano.it/2014/12/18/cec-pac-addio ALLA migliore riforma italiana dal dopoguerra ad oggi/1284514/>

<http://www.indicepa.gov.it/documentale/index.php>

<http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snpen&id=/20160422/snpen@s40@a2016@n16622@tS.clean.pdf>

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

<http://www.lineaamica.gov.it/risposte/obbligo-utilizzo-pec-parte-un-ente-pubblico-non-territoriale>

<http://www.pergliavvocati.it/forum/viewtopic.php?f=2&t=124>

<https://www.postacertificata.gov.it/home/sospensione-servizio.dot>

<http://www.quotidianodiritto.ilsole24ore.com/art/penale/2016-04-21/penale-si-alluso-ampio-pec-200427.php?uuid=ACoIC2CD>

<http://www.repubblica.it/online/internet/mediamente/cocco/cocco.html>

<http://www.techeconomy.it/2016/03/14/10-cose-modificare-al-cad-favorire-lopenness/>

<https://www.key4biz.it/nuovo-cad-i-rilievi-delle-regioni-troppi-dettagli-tecnici/150231/>

<http://www.wired.it/economia/lavoro/2014/03/03/posta-elettronica-certifica-abolire-petizione-change-org/>

<http://www.wired.it/economia/lavoro/2014/03/03/posta-elettronica-certifica-abolire-petizione-change-org/>