INAIL

Il Documento Informatico. Le diverse forme di sottoscrizione e trasmissione.

Riflessi sull'attività della Pubblica Amministrazione

Edizione maggio 2013

Pubblicazione realizzata da
INAIL
Avvocatura Generale

AUTORE
Vito Zammataro, *Responsabile settore finanziario, beni mobili e sviluppo procedure informatiche, Avvocatura Generale INAIL*

COLLABORAZIONE E CONSULENZA
Luigi La Peccerella, *Avvocato Generale INAIL*

CONTATTI
INAIL - Avvocatura Generale
via Pierluigi da Palestrina, 8 | 00193 Roma
Tel +39 06 5487 4856
avvocaturagenerale@inail.it
www.inail.it

ISBN 978-88-7484-302-2

Tipolitografia INAIL - Milano, maggio 2013

SOMMARIO

INTRODUZIONE

1. Il documento informatico e le diverse forme di sottoscrizione e trasmissione

1.1 Definizioni

L'art. 1 del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) fornisce una serie di definizioni che consentono una più agevole comprensione della terminologia utilizzata dal legislatore nella specifica materia; di seguito si evidenziano le più ricorrenti utilizzate nella presente trattazione:

- **documento informatico**: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
- **gestore di posta elettronica certificata**: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata;
- **posta elettronica certificata**: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;
- **firma elettronica**: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;
- **firma elettronica avanzata**: 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;
- **firma elettronica qualificata**: 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;
- **firma digitale**: 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;
- **chiave privata**: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;
- **chiave pubblica**: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;
- **certificati elettronici**: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;
- **certificato qualificato**: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;
- **certificatore**: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

- **pubbliche amministrazioni centrali**: le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, **gli enti pubblici non economici nazionali**, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;
- **titolare**: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;
- **validazione temporale**: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

1.2 Il documento informatico

L'art. 1 lett. p) del decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale) definisce il documento informatico come *"la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".
Nel testo del "Codice" - o in altre fonti, di rango primario e secondario, ivi richiamate - sono compendiati i requisiti in relazione ai quali viene riconosciuta la validità legale del documento informatico, distinguendo tra quello non firmato e quello firmato e tenendo conto, nel secondo caso, del tipo di firma elettronica impiegata. Il Codice specifica, inoltre, le modalità di conservazione, trasmissione ed utilizzo del documento informatico che ne garantiscono autenticità, integrità, provenienza e certezza di invio/ricezione.
Per quanto attiene alla loro validità legale, i documenti informatici sono distinti in tre categorie:
- documento non firmato;
- documento firmato con firma elettronica;
- documento firmato con firma elettronica avanzata: qualificata o digitale.

1) **Documento informatico non firmato**
L'articolo 23-quater del Codice dell'amministrazione digitale ha modificato l'articolo 2712 del codice civile, aggiungendo le riproduzioni informatiche alle altre forme di riproduzione, registrazione e rappresentazione meccanica delle quali il predetto articolo disciplina la validità legale.
Per effetto di tale modifica, le riproduzioni informatiche *"formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime*".
La limitata valenza probatoria del documento informatico non firmato, di cui al citato art. 2712 c.c., presuppone, comunque, per quanto riguarda i testi scritti, l'esistenza di un documento cartaceo di cui quello informatico costituisca la fedele riproduzione. Per quanto riguarda, invece, immagini e suoni la valenza probatoria di cui all'art. 2712 c.c. è attribuibile anche quando il formato digitale è nativo.

2) **Documento informatico firmato con firma elettronica**
Il Codice dell'amministrazione digitale definisce la firma elettronica come *"l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica*".
Quale esempio di firma elettronica di ampia diffusione si può citare l'abbinamento di PIN e Password.

L'associazione di un documento informatico a determinate PIN e Password consente di attribuire il documento stesso al soggetto che risulta essere titolare delle predette credenziali di identificazione informatica.
L'attribuzione del documento, peraltro, può essere inficiata da dubbi in merito alla reale identità del soggetto al quale sono associate le credenziali o in merito alle garanzie di sicurezza atte ad impedire che le credenziali stesse possano essere conosciute ed utilizzate da parte di soggetti diversi dal titolare. Le credenziali di identificazione informatica, inoltre, non sono, di per se stesse, idonee a garantire che il documento informatico non sia oggetto di manipolazioni e modifiche successive alla sua formazione ed associazione con la firma elettronica semplice.
Per queste ragioni l'articolo 21, comma 1, del codice dell'amministrazione digitale dispone che *"il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità*".
In conclusione, la tipologia di documenti in esame, pur non essendo priva di rilevanza giuridica, è tuttavia soggetta, quanto al suo valore probatorio ed alla sua idoneità a soddisfare il requisito della forma scritta, a valutazione e giudizio in ordine alle garanzie assicurate dalle concrete modalità di volta in volta applicate per la generazione, l'attribuzione e l'utilizzazione della firma elettronica.

3) **Documento informatico firmato con firma elettronica avanzata: qualificata o digitale**
Ai sensi della legislazione vigente la firma elettronica è "avanzata" quando:
- è univocamente connessa al firmatario;
- è creata con mezzi sui quali il firmatario può conservare un controllo esclusivo;
- consente di rilevare se i dati ai quali è connessa siano stati modificati successivamente all'apposizione della firma.

Il documento sottoscritto con firma elettronica avanzata integra il requisito della forma scritta per tutti gli atti e i contratti, di cui all'art. 1350 c.c., che richiedano la forma scritta *ad substantiam* per la loro validità ad eccezione per quelli aventi ad oggetto beni immobili.

La firma elettronica avanzata (semplice) non richiede necessariamente un dispositivo di firma. Un tipico esempio di tale tipologia di firma si rinviene nel caso di **firma c.d. "grafometrica**", cioè della sottoscrizione autografa apposta su *tablet* informatico con una penna specificamente dedicata; in questa ipotesi, poiché viene utilizzata la mano, non sussiste alcun dispositivo di firma.
A seguito delle modifiche apportate all'art. 21 del "Codice", (dall'art. 1, comma 1, del D.Lgs. 30 dicembre 2010 n. 235 prima, e, successivamente dall'articolo 9, comma 1, del D.L. 18 ottobre 2012 n. 179), ed alla luce di quanto sopra detto, il disconoscimento del documento informatico con firma elettronica avanzata non è più basato sulla prova del mancato utilizzo del dispositivo di firma da parte del titolare. Il mancato utilizzo del dispositivo di firma, che comporta il disconoscimento del documento informatico, con relativa inversione dell'onere probatorio, è ora limitato alla firma elettronica qualificata o digitale.

> La **firma elettronica qualificata** è un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.
> La **firma digitale** è un particolare tipo di firma elettronica avanzata basata su un sistema di

chiavi crittografiche, una pubblica e una privata, correlate tra di loro ed è rilasciata da un certificatore qualificato, che garantisce l'identità del titolare della firma.
La **chiave privata** è nota soltanto al titolare della firma ed è dallo stesso utilizzata per firmare il documento. L'apposizione della firma genera, per mezzo della funzione crittografica di hash, una stringa di dimensione fissa (la c.d. **impronta di hash**), indipendentemente dalla lunghezza del documento, che contiene i dati del documento stesso e quelli del certificato di firma digitale.

La **firma elettronica** qualificata è un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.
La **firma digitale** è un particolare tipo di firma elettronica avanzata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra di loro ed è rilasciata da un certificatore qualificato, che garantisce l'identità del titolare della firma.
La **chiave privata** è nota soltanto al titolare della firma ed è dallo stesso utilizzata per firmare il documento. L'apposizione della firma genera, per mezzo della funzione crittografica di hash, una stringa di dimensione fissa (la c.d. **impronta di hash**), indipendentemente dalla lunghezza del documento, che contiene i dati del documento stesso e quelli del certificato di firma digitale.
Per mezzo della **chiave pubblica**, che è disponibile per chiunque vi abbia interesse, ma che non può, ovviamente, generare la firma, è possibile verificare l'identità del soggetto che ha firmato il documento ed accertarsi che il documento stesso non sia stato modificato dopo l'apposizione della firma; anche la più piccola modifica del documento, infatti, causerebbe una alterazione dell'impronta.
La firma elettronica qualificata e la firma digitale richiedono, pertanto, una necessaria mediazione tecnologica: un "dispositivo" di firma che si sostituisca alla mano per apporre la firma.
L'utilizzo del dispositivo di firma, inoltre, si presume riconducibile al titolare, salvo che questi dia prova contraria.
La **firma digitale** adottata dall'Italia garantisce, perciò, l'autenticità, la non ripudiabilità e l'integrità del documento informatico, nel senso che è certa e verificabile l'identità del soggetto al quale il documento è attribuito, colui che ha firmato il documento non può disconoscerlo ed è sempre possibile verificare, in virtù dell'impronta di hash, che il documento stesso non sia stato modificato dopo l'apposizione della firma.
In considerazione, appunto, delle garanzie offerte dalla firma digitale, l'articolo 21, comma 2, del Codice dell'amministrazione digitale dispone che *"il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale …… ha l'efficacia prevista dall'articolo 2702 del codice civile".*
Il documento informatico sottoscritto con firma elettronica qualificata o digitale ha, pertanto, lo stesso valore della scrittura privata riconosciuta o autenticata e fa piena prova fino a querela di falso.
La validità legale del documento informatico così firmato rimane inalterata anche in caso di utilizzazione di software che - come accade, ad esempio, con HSM (Hardware Security Module) - assista l'utente nel processo di apposizione della firma digitale, facilitando, tra l'atro, la **firma massiva di documenti**; ciò sempre che, ovviamente, il software utilizzato abbia caratteristiche tali da garantire che i dati del certificato digitale di firma non siano accessibili da parte di soggetti diversi dal titolare.
L'utilizzo di HSM è particolarmente utile nel caso in cui il procedimento di sottoscrizione coinvolga un elevato numero di documenti, non essendo efficiente la sottoscrizione "documento

per documento", quanto meno perché ogni sottoscrizione richiede la digitazione del PIN di sblocco della smart card di firma.
In questi casi si potranno utilizzare procedure automatiche di sottoscrizione, purché ci si attenga alle prescrizioni dettate dalla legislazione vigente, cui si è fatto sopra cenno.
In particolare, è necessario che quando il titolare appone la sua firma mediante una procedura automatica utilizzi una coppia di chiavi diversa da tutte le altre in suo possesso. Questo per identificare immediatamente, in fase di verifica, il fatto che è stata utilizzata una procedura automatica. Per motivi analoghi, ogni dispositivo di firma utilizzato per procedure automatiche deve disporre di coppie di chiavi differenti, una per dispositivo, anche se il titolare è sempre lo stesso.
È anche possibile utilizzare particolari applicazioni che consentono di digitare il PIN una sola volta a fronte della sottoscrizione di più documenti, garantendo comunque una chiara informativa circa la natura ed il numero dei documenti che verranno automaticamente sottoscritti.
Quale che sia la modalità di apposizione della firma digitale, con o senza assistenza di peculiari software, il valore giuridico del documento sottoscritto è connesso alle sue caratteristiche intrinseche di autenticità, non ripudiabilità ed integrità, verificabili per mezzo della c.d. **impronta di hash**, sicché il documento stesso conserva il suo pieno valore indipendentemente dalle modalità di trasmissione telematica.
Gli artt.26 e 27 del CAD definiscono la figura e disciplinano l'attività dei **Certificatori.** Questi soggetti, operando nel rispetto della vigente normativa in materia di firma digitale e delle regole tecniche emanate dal CNIPA *(ora Agenzia per l'Italia Digitale),* garantiscono l'identità dei soggetti che utilizzano la firma digitale, e, pertanto, al fine di fornire protezione nei confronti di possibili danni derivanti da un esercizio non adeguato delle attività di certificazione, devono possedere particolari requisiti tecnici, organizzativi e societari.
I Certificatori svolgono, tra gli altri, i seguenti compiti fondamentali:

- verificano ed attestano, emettendo un apposito certificato digitale, l'identità del titolare ed eventualmente la veridicità di una serie di altre informazioni;
- stabiliscono il termine di scadenza dei certificati;
- pubblicano il certificato e la chiave pubblica;
- ricevono la segnalazione di eventuali smarrimenti, furti, cancellazioni, divulgazioni improprie di chiavi private e pubblicano quindi la lista dei certificati revocati o sospesi in conseguenza di tali fatti.

L'Ente Certificatore deve:

- provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;
- specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;
- attenersi alle regole tecniche prescritte dalla normativa in materia;
- informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione; non rendersi depositario di dati per la creazione della firma del titolare;
- garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo

nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;
- non copiare, né conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione.

Per il suo funzionamento l'utente deve essere dotato di un apposito kit costituito da una smart card, da un lettore di smart card e da un software di firma. In alternativa alla smart card l'utente può utilizzare un token USB (chiavetta).

> Le Smart Card e i token USB - dispositivi di firma utilizzati per la firma digitale e i servizi di identificazione - sono apparati elettronici in grado di conservare in maniera protetta le chiavi private e di generare al loro interno la firma digitale. Utilizzano microprocessori basati su standard previsti dalla legge, nei quali sono implementate avanzate tecnologie crittografiche in un ambiente con standard di sicurezza molto elevati.
> I requisiti necessari per richiedere all'Ente Certificatore un dispositivo di firma digitale sono:
> • aver compito 18 anni;
> • essere in possesso del codice fiscale;
> • essere in possesso di un documento di identità in corso di validità.
> Per agevolare la diffusione della firma digitale, sono previste specifiche modalità di rilascio per le imprese e le pubbliche amministrazioni che debbano dotare propri dipendenti del dispositivo di firma.
> In questo caso, l'impresa, o la pubblica amministrazione, dovrà rivolgersi ad uno dei certificatori accreditati per scegliere, sulla base del numero dei kit necessari, del costo complessivo dell'operazione e dei servizi accessori offerti, quello che meglio soddisfa le proprie esigenze. Peraltro, è possibile demandare all'impresa, o pubblica amministrazione, richiedente l'attività di registrazione e di verifica dell'identità del titolare del certificato, ogni qualvolta ciò comporti benefici a tutti i soggetti coinvolti (dipendente, datore di lavoro e certificatore). In tale ipotesi il dipendente non deve recarsi fisicamente presso l'autorità di registrazione del certificatore, l'impresa, o la P.A., richiedente ha un controllo diretto dei certificati emessi per i propri dipendenti con procedure snelle e rapide che consentono di richiedere, all'occorrenza, sospensioni e revoche dei certificati stessi. Il certificatore non deve impegnare risorse umane per il riconoscimento dei titolari, la verifica dei titoli e di eventuali incarichi o ruoli svolti per il richiedente.
> Le pubbliche amministrazioni possono anche richiedere di essere accreditate (iscritte quindi nell'elenco pubblico dei certificatori) utilizzando in realtà le infrastrutture tecnologiche di uno dei soggetti già iscritti nell'elenco pubblico dei certificatori. In questo caso, ottengono l'ulteriore vantaggio di risultare, nella fase di verifica di un documento informatico sottoscritto con firma digitale da un proprio dipendente, quali soggetti che emettono e garantiscono le informazioni inerenti il dipendente stesso e di esercitare un maggiore controllo sulle attività di certificazione.

Attraverso questi strumenti l'utente ha la possibilità di applicare la propria firma digitale e la marca temporale su qualunque documento informatico.
La **validazione - o marca - temporale** è il risultato di una procedura informatica che consente di attribuire a un documento informatico una data e un orario opponibile ai terzi.
Dal punto di vista operativo, il servizio di marcatura temporale di un documento informatico consiste nella generazione, da parte di un soggetto terzo, di una firma digitale del documento cui è associata l'informazione relativa a una data e a un'ora certa.

Un file marcato temporalmente contiene il documento del quale si è chiesta la validazione temporale e la marca emessa dall'ente certificatore.

Inoltre, tutte le marche temporali vengono conservate in un apposito archivio per un periodo non inferiore a venti anni ovvero, su richiesta dell'interessato, per un periodo maggiore.
Il limite che tale sistema di sottoscrizione presenta riguarda la validità dei documenti informatici nel tempo, nel senso che, essendo la firma digitale subordinata alla validità (solitamente triennale) di uno specifico certificato qualificato, alla scadenza di quest'ultimo i documenti rischiano di non essere più validi.
Per ovviare a tale problema, occorre apporre sui documenti informatici una marca temporale prima della scadenza del certificato.
Quindi la firma digitale, anche se il relativo certificato qualificato risulti scaduto, revocato o sospeso, è valida se alla stessa è associabile un riferimento temporale opponibile ai terzi che colloca la generazione di detta firma in un momento precedente alla scadenza, sospensione o revoca del certificato.
In pratica, se dopo aver firmato digitalmente un documento vi si appone anche una marca temporale, si rende la firma digitale valida nel tempo.
Il tempo, cui fanno riferimento le marche temporali, è riferito al Tempo Universale Coordinato, ed è assicurato da un ricevitore radio sintonizzato con il segnale emesso dall'Istituto Elettrotecnico Nazionale Galileo Ferraris.

L'attività dei certificatori e dei gestori di posta elettronica certificata, in considerazione della rilevante funzione svolta, è soggetta alla vigilanza ed al controllo dell'Agenzia per l'Italia Digitale.
Qualora si verifichi un **disservizio o un malfunzionamento nel sistema** che determini l'interruzione del servizio, il certificatore qualificato o il gestore di posta elettronica certificata deve darne tempestiva comunicazione agli utenti o all'Agenzia; quest'ultima, salvo i casi di forza maggiore o di caso fortuito, provvederà a diffidare il certificatore qualificato o il gestore di posta elettronica certificata a ripristinare la regolarità del servizio o ad effettuare le dovute comunicazioni, se omesse o non tempestive. Se il disservizio o l'interruzione del servizio, ovvero la mancata o intempestiva loro comunicazione, sono reiterati, rispettivamente, per due volte, in caso di disservizio, o una volta, in caso di interruzione, nel corso di un biennio, successivamente alla seconda o alla prima diffida si applica la sanzione della cancellazione dall'elenco pubblico.
In ogni caso può essere applicata la sanzione amministrativa accessoria della pubblicazione dei provvedimenti di diffida o di cancellazione secondo la legislazione vigente in materia di pubblicità legale.
Qualora un certificatore qualificato o un gestore di posta elettronica certificata non ottemperi, nei tempi previsti, a quanto prescritto dall'Agenzia nell'esercizio delle attività di vigilanza si applica la sanzione della cancellazione dall'elenco pubblico successivamente alla prima diffida.

1.3 L'utilizzazione dei documenti informatici: valore probatorio

L'art. 20 del "Codice" prevede, in generale, la validità e la rilevanza agli effetti di legge del documento informatico da chiunque formato, della sua memorizzazione su supporto informatico e della trasmissione con strumenti telematici conformi alle regole tecniche.

Pertanto, il documento "dematerializzato", qualora rispetti le regole tecniche fissate dalla normativa vigente, ha il medesimo valore legale e probatorio del documento cartaceo (o analogico in genere) e deve essere accettato da qualsiasi soggetto pubblico o privato.

Il principio generale, espresso nel comma 1-bis dall'art. 20, prevede che l'idoneità del documento informatico a soddisfare il requisito della forma scritta ed il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità.
Diversa è l'ipotesi del documento informatico sottoscritto. In questa ipotesi, infatti, l'art. 21 del CAD individua il diverso valore probatorio riconosciuto al documento informatico in ragione della tipologia di firma apposta. Analogamente a quanto previsto per i documenti analogici (cartacei), infatti, la sottoscrizione è l'elemento discriminante che permette di attribuire all'autore la paternità giuridica del documento.
Ciò posto, la dematerializzazione dei documenti, processo attraverso il quale il documento giuridico viene formato e conservato utilizzando supporti di natura informatica, è, dunque, un processo ormai ineluttabile della nostra quotidianità.
La dematerializzazione riguarda sia i documenti che vengono creati direttamente in formato digitale sia le conversioni (copie) analogico/digitale ed investe tutti i documenti di cui la legge impone la conservazione.
Ai fini dell'attività amministrativa assume, quindi, grande rilevanza la disciplina dettata dal Codice in materia di documento informatico e di copie degli atti e dei documenti informatici (Capo II, Sez. I, II, artt.20/37 - C.A.D).
Il CAD introduce, pertanto, le definizioni di copie e duplicati informatici che sono utilizzate per disciplinare la complessa questione della copia di un documento su un supporto differente da quello originale:

- copia informatica di documento analogico (cartaceo);
- copia analogica (cartacea) di documento informatico;
- copia informatica di un documento informatico e duplicato informatico.

- Copia informatica di documento analogico (cartaceo)
La "*copia informatica di documento analogico*" (art. 1, comma 1, lett. i-bis CAD) è definita come il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto.

L'art. 22, comma 1, dispone che le copie informatiche di documenti analogici, spedite o rilasciate dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno la medesima efficacia probatoria degli originali se ad esse è apposta o associata, da parte di colui che le spedisce o rilascia, una firma digitale o altra firma elettronica qualificata.
I documenti conformi a queste prescrizioni sostituiscono, a tutti gli effetti, gli originali. Questo principio si applica anche alle copie su supporto informatico dei documenti formati in origine su supporto cartaceo dalla pubblica amministrazione: tali copie hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la conformità all'originale è assicurata, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata, dal funzionario delegato.

La "*copia per immagine su supporto informatico di documento analogico*" (art. 1, comma 1,

lett. i-ter) è definita come il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto. **Si tratta, per esempio, del documento .pdf che risulta dalla scansione di un documento analogico.**
L'art. 22, comma 2 e comma 3, dispone che le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la medesima efficacia probatoria degli originali se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71, o ancora, se sono formate nel rispetto delle regole tecniche di cui all'articolo 71 e la loro conformità all'originale non è espressamente disconosciuta.
Il comma 4, infine, dispone che le copie formate ai sensi dei precedenti commi sostituiscono ad ogni effetto di legge gli originali cartacei e sono idonee ad assolvere gli obblighi di conservazione disposti dalla legge.
L'articolo in commento costituisce il fondamento giuridico dell'archiviazione sostitutiva e, quindi, della dematerializzazione degli archivi, specificamente disciplinata dai successivi articoli 42, 43, 44 e 44-bis.
Tra i documenti originati in formato cartaceo che possono essere sostituiti da copia informatica devono essere annoverati anche gli atti predisposti tramite i sistemi informativi automatizzati, con firma autografa sostituita dall'indicazione a stampa, sul documento prodotto dal sistema automatizzato, del nominativo del soggetto responsabile, ai sensi dell'articolo 3 del D.Lgs. 12 febbraio 1993, n. 39.
Tale tipologia di documenti, pertanto, può trasmessa o per mezzo della posta ordinaria nel formato cartaceo risultante dalla stampa prodotta dal sistema informativo automatizzato, quale risultato finale dell'elaborazione, oppure a mezzo della posta elettronica nel formato della copia informatica del documento analogico.

- Copia analogica (cartacea) di documento informatico
L'art. 23 si occupa delle copie analogiche di documenti informatici, quindi per esempio, delle stampe cartacee di un documento informatico.
Si dispone che:
- **le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato;**
- **se manca la dichiarazione di conformità, le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta.**

Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

Il "Codice" prevede un regime differenziato per le copie analogiche (cartacee) dei documenti amministrativi digitali in ragione dei destinatari dei documenti stessi.
Con riguardo alle comunicazioni tra amministrazione e cittadino (cfr. par.3.1) l'art. 3-bis del CAD stabilisce che l'invio di comunicazioni da parte delle amministrazioni pubbliche, sotto forma di documenti informatici, a cittadini che non abbiano indicato il proprio domicilio digitale, possa avvenire attraverso l'invio di una copia analogica dei documenti

stessi, sottoscritta con firma autografa sostituita a mezzo stampa conformemente alle previsioni di legge (D.Lgs. 12 dicembre 1993, n. 39). L'amministrazione che invia copia cartacea della comunicazione redatta in originale informatico dovrà apporre una dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto e conservato presso l'amministrazione in conformità alle regole tecniche. Non è possibile, però, utilizzare questa procedura quando il documento inviato dall'amministrazione rappresenti, per propria natura, una certificazione da utilizzarsi nei rapporti tra privati.
Al di fuori di questa ipotesi trovano applicazione le regole generali (art. 23 CAD) che attribuiscono la stessa efficacia probatoria dell'originale da cui sono tratti alle copie analogiche di documenti informatici, quando la loro conformità al documento sorgente, in tutte le sue componenti, sia attestata da un pubblico ufficiale autorizzato.
Il soggetto che abbia richiesto ed ottenuto il rilascio di un documento informatico firmato con firma digitale, contenente, ad esempio, una dichiarazione o una certificazione, qualora non possa avvalersi per la sua utilizzazione di mezzi di trasmissione telematica o debba necessariamente esibirlo in forma cartacea, dovrà recarsi presso un pubblico ufficiale abilitato al rilascio di copie autentiche, esibendo il documento su supporto informatico; il pubblico ufficiale, verificata per mezzo della chiave pubblica l'autenticità e l'integrità del documento, rilascerà le copie autentiche, attestando la conformità all'originale informatico delle stampe su supporto cartaceo.

- Copia informatica di un documento informatico e duplicato informatico.
La "*copia informatica di documento informatico*" (art. 1, comma 1, lett. i-quater CAD) è definita come il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari.
In questo caso, pur restando invariati i fatti giuridicamente rilevanti rappresentati nel documento, varia il formato del file.
Si tratta, per esempio, del documento .pdf che risulta dalla effettuazione di una copia, cioè dalla registrazione in un diverso formato, di un documento .doc.

Il "*duplicato informatico*" (art. 1, comma 1, lett. i-quinquies) è definito come il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario.
Con questa espressione, pertanto, la normativa individua i documenti informatici che, oltre a rappresentare gli stessi atti o fatti giuridicamente rilevanti (quindi i contenuti del documento), mantengono il medesimo formato del file originale.
Si tratta, per esempio, della duplicazione di un documento .doc in un altro documento .doc.

L'art. 23-bis del CAD, sancisce che, se prodotti in conformità alle regole tecniche di cui al successivo art. 71:
- i duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti;
- le copie e gli estratti informatici del documento informatico, hanno la stessa efficacia probatoria dell'originale da cui sono tratti se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta.

Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

1.4 Gli atti formati dalla pubblica amministrazione

Art. 23 ter - documenti amministrativi informatici

In attesa della generalizzata e capillare diffusione della tecnologia informatica, al fine di rendere più agevole l'utilizzo dei documenti informatici si è fatto ricorso al Timbro Digitale (o glifo), verificato e sperimentato anche dall'Agenzia per l'Italia Digitale ed attualmente adottato da numerose pubbliche amministrazioni.
L'art. 23-ter, comma 5, del CAD ha, infatti, previsto un ulteriore strumento in grado di assicurare la conformità del documento stampato al documento amministrativo informatico originale.
In particolare, l'amministrazione che rilascia copia cartacea di documenti amministrativi informatici, per assicurarne la provenienza e la conformità con l'originale informatico da cui è tratta, può apporvi un contrassegno generato elettronicamente e riportato in formato stampa che consente la verifica automatica della conformità del documento analogico alla sorgente informatica.
Il contrassegno (Timbro digitale o Glifo),- è un codice a barre bidimensionale, generato con metodologie e strumenti open-source, che contiene non soltanto l'immagine originale del documento ma anche tutte le informazioni sulla firma digitale e sulla marca temporale, necessarie per la verifica dell'autenticità e dell'integrità. Il glifo, apposto sul documento informatico e riportato sulla versione stampata su supporto cartaceo, costituisce una rappresentazione convenzionale di informazioni contenute nel documento informatico stampabile, riconoscibile con strumenti elettronici, ottenuta utilizzando una codifica grafica definita, secondo le regole tecniche a suo tempo dettate dal **DPCM del 30 marzo 2009 n. 38840 e dalla Deliberazione CNIPA 21 maggio 2009, n. 45, come modificata ed integrata dalla Determinazione Commissariale DIGIT.PA n. 69 del 28 luglio 2010, ed ora riformulate dal DPCM del 22 febbraio 2013, n. 68380 (in G.U. n. 117/2013).**
Il soggetto al quale viene esibito il documento cartaceo può verificarne la conformità all'originale informatico leggendo il glifo con uno scanner e decodificandolo per mezzo di apposito software scaricabile gratuitamente.
L'estrazione così effettuata del documento originale e delle informazioni relative alla firma consente, pertanto, di ottenere conferma in ordine all'attendibilità del documento e di evidenziare eventuali difformità tra la versione stampata e l'originale informatico.
Il Timbro digitale o Glifo, inoltre, sostituisce a tutti gli effetti di legge la sottoscrizione autografa del documento amministrativo da parte del funzionario incaricato. Il cittadino non può richiedere all'amministrazione che consegna un documento amministrativo cartaceo cui sia apposto il contrassegno, la consegna di un'altra copia analogica del medesimo documento informatico con sottoscrizione autografa.
I software necessari per poter effettuare la verifica di conformità della copia cartacea all'originale informatico attraverso il contrassegno, devono essere gratuiti e messi liberamente a disposizione da parte delle amministrazioni.
L'utilizzazione del timbro digitale, inoltre, permette all'amministrazione di avvalersi, per la consegna del documento, anche dei tradizionali mezzi di trasmissione, rilasciando, all'occorrenza, il documento già su supporto cartaceo, in tal modo raggiungendo anche utenti non registrati nel portale o non dotati di casella di posta elettronica o il cui indirizzo telematico non sia noto all'Istituto.

1.5 La trasmissione dei documenti informatici

Per quanto riguarda, in generale, la trasmissione di documenti, il Codice dell'amministrazione

digitale riconosce la validità di qualsiasi mezzo telematico o informatico, ivi compreso il fax, purché idoneo ad accertarne la fonte di provenienza.
Con riferimento ai documenti informatici, il mezzo di trasmissione di elezione è costituito dalla posta elettronica.
Quale che sia la tipologia di posta elettronica utilizzata per la trasmissione, è comunque applicabile il principio di diritto secondo il quale il documento informatico trasmesso per via telematica si intende spedito dal mittente al momento dell'invio al proprio gestore, e si intende consegnato al destinatario nel momento in cui è reso disponibile nella casella di posta elettronica dello stesso.
Quanto al valore probatorio, invece, sono molto rilevanti le differenze di regime giuridico tra la posta elettronica ordinaria e quella certificata.

A) **Posta elettronica ordinaria**
L'autenticità del messaggio di posta elettronica ordinaria e dei documenti informatici allegati, che non siano firmati con firma digitale, è garantita esclusivamente dalle credenziali di identificazione informatica necessarie per l'accesso al servizio.
Le predette credenziali, peraltro, in nessun modo assicurano l'integrità del messaggio e dei suoi allegati, anche quando siano atti predisposti con sistemi automatizzati e per i quali, ai sensi dell'articolo 3 del D.Lgs. 12 febbraio 1993, n. 39, la firma autografa è validamente sostituita dall'indicazione a stampa del nominativo del soggetto responsabile
La posta elettronica ordinaria, inoltre, non è idonea a fornire certezza della data di spedizione e di quella di avvenuta ricezione.
Per queste ragioni i messaggi di posta elettronica ordinaria hanno, al più, il valore probatorio di cui all'articolo 2712 c.c., di cui si è detto in precedenza.

B) **Posta elettronica certificata**
La Posta Elettronica Certificata (PEC) è compiutamente disciplinata dal Codice dell'amministrazione digitale e dal d.P.R. 11 febbraio 2005, n. 68, che la indicano quale unico mezzo valido ai fini della trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna.
Le caselle di posta elettronica certificata sono rilasciate da **gestori** del servizio, iscritti in apposito elenco tenuto dall'Agenzia per l'Italia Digitale previa verifica del possesso dei requisiti soggettivi ed oggettivi prescritti dalla legge.
Il gestore accerta e verifica l'identità del soggetto al quale è rilasciata la casella PEC, sicché risulta garantita l'identità sia del mittente che del destinatario del messaggio. La validità legale della posta elettronica certificata presuppone, infatti, che sia la casella del mittente che quella del destinatario siano caselle PEC.
Quando è inviato un messaggio, il gestore della casella di PEC del mittente inoltra allo stesso una ricevuta che costituisce prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata, oltre che della data di spedizione. Allorché il messaggio perviene al destinatario, cioè è reso disponibile nella sua casella di PEC, il gestore invia al mittente la ricevuta di avvenuta (o mancata) consegna, con precisa indicazione temporale. Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte, conservata per legge per un periodo di 30 mesi, consente la riproduzione, con lo stesso valore giuridico, delle ricevute stesse.
La PEC, quindi, garantisce l'autenticità del messaggio e la data certa di spedizione e di ricezione.

Il gestore, infatti, appone in automatico sulla busta di trasporto, contenente il messaggio e gli allegati, oltre che sulle ricevute, la propria firma elettronica qualificata (solitamente digitale); in tal modo è garantita anche l'integrità del messaggio e degli allegati, sempre che sia rilasciata la ricevuta completa, di cui si dirà di seguito.
Ne consegue che anche il documento informatico non firmato, contenuto nella busta di trasporto e che nel testo del messaggio il mittente afferma essergli attribuibile, assume pieno valore probatorio; ciò vale anche quando il documento allegato sia un atto predisposto con sistemi automatizzati, recante, in luogo della sottoscrizione autografa, l'indicazione del nominativo del responsabile.
Se invece il mittente attribuisce il documento non firmato, allegato al messaggio, ad un soggetto terzo, la PEC costituirà piena prova del fatto che il mittente ha effettivamente inviato quel documento in allegato e che lo ha attribuito ad un determinato soggetto, ma non prova che il documento stesso sia realmente riconducibile al soggetto indicato dal mittente.
In relazione con quanto sopra indicato, il **gestore** può emettere, quindi, tre differenti tipologie di ricevute di avvenuta consegna, che possono soddisfare differenti esigenze dell'utenza:

- la r**icevuta completa** è costituita da un messaggio di posta elettronica inviato al mittente che riporta in formato leggibile i dati di certificazione (mittente, destinatario, oggetto, data e ora di avvenuta consegna, codice identificativo del messaggio). Gli stessi dati sono inseriti all'interno di un file XML allegato alla ricevuta. Per le consegne relative ai destinatari primari del messaggio (che sono i destinatari diretti del messaggio diversi dai destinatari riceventi in copia), la ricevuta di avvenuta consegna contiene anche il messaggio originale, testo ed eventuali allegati.

Il gestore, nelle ipotesi in cui l'utente utilizza la ricevuta completa, garantisce, oltre l'integrità del messaggio, anche l'integrità dei documenti eventualmente allegati, anche se non firmati digitalmente:

- la **ricevuta breve** ha lo scopo di ridurre i flussi di trasmissione della Posta Elettronica Certificata, soprattutto in quei casi in cui la mole di documenti e di messaggi scambiati è consistente. Per questo, la ricevuta breve contiene il messaggio originale e gli hash crittografici degli eventuali allegati. Per permettere la verifica dei contenuti trasmessi, il mittente deve conservare gli originali non modificati degli allegati inseriti nel messaggio originale a cui gli hash fanno riferimento;
- la **ricevuta sintetica** segue le regole di emissione della ricevuta completa solo che l'allegato contiene esclusivamente il file XML con i dati di certificazione descritti. La ricevuta sintetica è particolarmente utile per i servizi che includono la Posta Elettronica Certificata come strumento di trasporto a supporto di una forte automazione dei flussi di comunicazione.

La trasmissione dei documenti informatici, infine, è soggetta ad un diverso regime giuridico quando integrata nel contesto della cooperazione applicativa e del sistema pubblico di connettività di cui agli articoli 63 e seguenti del Codice.
L'articolo 76 dispone, infatti che "*gli scambi di documenti informatici tra le pubbliche amministrazioni nell'ambito del SPC, realizzati attraverso la cooperazione applicativa e nel rispetto delle relative procedure e regole tecniche di sicurezza, costituiscono invio documentale valido ad ogni effetto di legge*".
In questo contesto è anche possibile che il sistema informatico di una pubblica amministrazione interagisca non già con un singolo utente, ma con una entità organizzata, anche di diritto privato, anch'essa dotata di un sistema informatico.

In tale caso il dialogo avviene tra le porte di dominio dei due sistemi e l'autenticazione, non più dei singoli soggetti ma delle due persone giuridiche, è asseverata dai certificati digitali delle predette porte di dominio (v. infra par.3.3).

I - PARTE GENERALE

2. Quadro normativo di riferimento

Sul finire degli anni '90 sono stati emanati diversi provvedimenti legislativi che hanno conferito valore giuridico al documento informatico ed alla firma digitale, ma è con la pubblicazione della Direttiva 1999/93/CE che è stata impressa una accelerazione al processo legislativo.
Il legislatore comunitario, oltre ad imporre un quadro comune agli Stati dell'Unione Europea, ha dettato i criteri tecnologici da utilizzare per equiparare, da un punto di vista giuridico, le firme digitali a quelle autografe.
La prima norma che ha, invece, espressamente fatto menzione della posta elettronica certificata si rinviene, in Italia, nella legge 16 gennaio 2003, n. 3, recante disposizioni ordinamentali in materia di pubblica amministrazione.
In particolare, l'art. 27, tra l'altro, ha individuato la Posta Elettronica Certificata - PEC - come uno degli elementi fondamentali per perseguire per una maggiore efficienza ed economicità dell'azione amministrativa nonché la modernizzazione e lo sviluppo del paese.
Si illustrano di seguito le principali disposizioni legislative e regolamentari che documentano, cronologicamente, l'evoluzione normativa dell'ultimo decennio in concomitanza allo sviluppo tecnologico dell'informatica.

- Direttiva europea 1999/93/CE sulle firme elettroniche - *"Directive 1999/93/EC of the European Parliament and of the Council on a common framework for electronic signatures";*

  La normativa dettata dal legislatore comunitario ha introdotto differenti livelli di sottoscrizione. Nel linguaggio corrente, sono stati utilizzati i termini firma "debole" e firma "forte".
  Il legislatore definisce digitale la firma cd. "forte", in quanto basata su un sistema a chiavi crittografiche asimmetriche ed utilizza un certificato digitale con particolari caratteristiche, rilasciato da un soggetto con specifiche capacità professionali garantite dallo Stato e viene creata mediante un dispositivo con elevate caratteristiche di sicurezza che in genere è una smart card.
  Tutto ciò che non risponde alle caratteristiche sopra descritte, ma, in ogni caso, è compatibile con la definizione giuridica di firma elettronica, viene, invece, definito firma "debole" o "leggera".
  L'efficacia giuridica delle due firme è diversa. La firma digitale è equivalente a una sottoscrizione autografa. Le altre potrebbero non esserlo: vengono valutate in fase di giudizio in base a caratteristiche oggettive di qualità e sicurezza.
  Come ulteriore garanzia per la pubblica amministrazione, che è obbligata ad accettare i documenti firmati digitalmente, i certificatori che intendono rilasciare certificati digitali validi per le sottoscrizioni di istanze e dichiarazioni inviate per via telematica alla pubblica amministrazione stessa, possono dimostrare di possedere particolari e comunque superiori caratteristiche di qualità e sicurezza e ottenere quindi la qualifica di "certificatore accreditato". Tale qualifica è sotto il controllo ed è garantita, in Italia, dallo Stato.

Pertanto, quando, in un documento informatico, si ha la necessità di una sottoscrizione equivalente a quella autografa è indispensabile utilizzare la firma digitale.
Negli altri casi di firma "debole" più che di un processo di firma si potrà riconoscere un processo di autenticazione con minori requisiti di sicurezza e quindi con una minore efficacia probatoria.
Nell'ambito della pubblica amministrazione, conseguentemente, l'espressione del potere di firma nel documento informatico da parte del funzionario che ne ha titolarità, dovrà essere esercitata con la firma digitale.

- Legge 21 gennaio 1994, n. 53 - "*Facoltà di notificazioni di atti civili, amministrativi e stragiudiziali per gli avvocati e procuratori legali*";

  La legge, nel corso degli anni, è stata oggetto di diverse modifiche ed integrazioni in concomitanza all'evoluzione della telematica applicata ai procedimenti giudiziari. Ad esempio, oggi, ai sensi dell'art. 4, l'avvocato, munito di procura e di specifica autorizzazione rilasciata dal Consiglio dell'Ordine di appartenenza, può eseguire notificazioni in materia civile, amministrativa e stragiudiziale, direttamente, anche a **mezzo posta elettronica certificata**.

- Decreto del Presidente della Repubblica 28 dicembre 2000 n. 45 - "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*";
- Decreto legislativo 23 gennaio 2002, n. 10 - "*Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche*" - **abrogato a decorrere dal 1° gennaio 2006, per effetto dell'articolo 75 del D.Lgs. 7 marzo 2005, n. 82**;
- Decreto del Presidente della Repubblica 7 aprile 2003, n. 137 - *"Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10"*;
- Legge 16 gennaio 2003 n. 3, *"Disposizioni ordinamentali in materia di pubblica amministrazione"*- art. 27;
- Decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003 n. 14142 - *"Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10";*
- Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 n. 14146 "*Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici*" **abrogato dall'articolo 53, comma 2, del D.P.C.M. 30 marzo 2009, n. 38840**;
- Deliberazione CNIPA (oggi Agenzia per l'Italia digitale, ex DigitPA) n. 4 del 17 febbraio 2005 *"Regole per il riconoscimento e la verifica del documento informatico"*;
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, *"Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3."*, disciplina le modalità di utilizzo della Posta Elettronica Certificata non solo nei rapporti con la PA, ma anche tra privati cittadini;

  In sintesi, la normativa ha previsto che:
  - Sia i privati, sia le Pubbliche Amministrazioni possono scambiarsi e-mail certificate. Saranno i gestori del servizio a fare da garanti dell'avvenuta consegna. I gestori sono iscritti

nell'apposito elenco tenuto da *Agenzia per l'Italia digitale* (ex DigitPA), che si occupa di verificare i requisiti inerenti per esempio alla capacità ed esperienza tecnico-organizzativa, alla dimestichezza con procedure e metodi per la gestione della sicurezza, alla certificazione ISO9000 del processo.

- Per iscriversi nell'elenco, i potenziali gestori devono possedere un capitale sociale minimo non inferiore a un milione di euro e presentare una polizza assicurativa contro i rischi derivanti dall'attività di gestore.
- I messaggi vengono sottoscritti automaticamente da parte dei gestori con firme elettroniche. Tali firme sono apposte su tutte le tipologie di messaggi di posta certificata PEC, per assicurare l'integrità e l'autenticità del messaggio.
- I gestori devono conservare traccia delle operazioni per 30 mesi.
- I gestori sono tenuti a verificare l'eventuale presenza di virus nelle e-mail e a informare in caso positivo il mittente, bloccandone la trasmissione.

- Decreto Legislativo 7 marzo 2005, n. 82 - C.A.D. (Codice dell'Amministrazione Digitale) Rinvio;
- Decreto Ministeriale 2 novembre 2005 n. 19818, *"Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata*", con Allegato *«Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata»;*

  - **validità temporale delle ricevute PEC.**

  La firma apposta elettronicamente è valida "*sine die*" se il certificato era in corso di validità al momento in cui è stata generata. Perché sia verificabile la validità del certificato al momento della firma, è necessario che questo sia **determinabile** in maniera sicura.

  Ad ogni singolo gestore possono essere, infatti, rilasciati fino ad un massimo di dieci certificati di firma e, qualora un gestore abbia ravvisato la necessità di utilizzare un numero di certificati di firma superiore a dieci, può richiederli all'*Agenzia per l'Italia digitale* (ex DigitPA) documentando tale necessità. L'AgID, previa valutazione della richiesta, stabilisce se fornire o meno al gestore ulteriori certificati di firma (cfr. art. 7, D.M. 2 novembre 2005 n. 19818).

  Le regole tecniche della PEC prevedono, quindi, la presenza di un riferimento temporale sicuro all'interno dei dati di certificazione di tutti i messaggi PEC (ricevute, buste di trasporto, ecc.) che, quando firmati digitalmente dal gestore, costituiscono prova opponibile a terzi. La ricevuta PEC costituisce un "*insieme*" che assicura contemporaneamente integrità, tempo, dati di trasporto e contenuto del messaggio originale (quest'ultimo elemento non è presente se il mittente ha esplicitamente richiesto una "ricevuta sintetica").

  Questo insieme, garantito dalla struttura S/MIME che lo contiene, consente quindi un'opponibilità a terzi nel tempo autoconsistente (anche successivamente alla scadenza del certificato di firma) senza necessità di ulteriori marcature temporali "esterne".

  Le ricevute (che hanno una propria marcatura temporale fidata e garantita) non scadono, anche se il certificato cessa di essere valido dopo che sono state emesse.

  Il DPR 68/2005 definisce all'art. 1 comma 1, lettera i) il riferimento temporale come *"l'informazione contenente la data e l'ora che viene associata ad un messaggio di posta elettronica certificata*". L'art. 10 rimanda alle regole tecniche (v. D.M. 2 novembre 2005) per la formazione dei riferimenti temporali e impone che questi siano inseriti in tutti i messaggi generati dai gestori PEC. Il DPR 68/2005 definisce inoltre i gestori PEC come terze parti fidate, in base ai requisiti per operare richiesti all'art. 14 comma 3 e segg.

Il D.M. 2 novembre 2005 all'art. 9 prevede, inoltre, l'unicità del riferimento temporale e prescrive che il gestore deve garantire adeguate misure affinché il riferimento temporale non possa differire di più di un secondo dal Riferimento Nazionale del Tempo Universale Coordinato (UTC). A tal fine l'art. 21, comma 1, lettera f), prevede una specifica figura di responsabile del *"sistema di riferimento temporale"*. L'importanza del riferimento temporale, per il buon funzionamento nel sistema PEC, è altresì evidenziata dall'art. 23 comma 3, lettera h) dove si prescrive che il manuale operativo del gestore PEC deve individuare le modalità di definizione del riferimento temporale. Le regole tecniche allegate al D.M. in esame definiscono puntualmente l'unicità transazionale del riferimento temporale usato per le ricevute, messaggi, log, ecc. Il riferimento temporale è inserito nelle ricevute sia in formato testuale a uso di un utente, sia in formato XML per elaborazioni automatiche.

Si crea, quindi, una struttura inalterabile (firma digitale del gestore) che contiene un riferimento temporale certo e affidabile (grazie ai requisiti tecnici e organizzativi) relativo all'istante della firma. In questo modo è garantita l'opponibilità a terzi della ricevuta firmata dal gestore che svolge il ruolo di terza parte fidata grazie ai requisiti normativi imposti dal legislatore che valgono tanto per il meccanismo di firma che per il riferimento temporale.

- Circolare CNIPA (oggi Agenzia per l'Italia digitale, ex DigitPA) n. 49 del 24 novembre 2005, *"Modalità per la presentazione delle domande di iscrizione all'elenco pubblico dei gestori di posta elettronica certificata*", stabilisce le modalità di accreditamento per i soggetti che vogliono svolgere il servizio di Gestore PEC
- Circolare CNIPA 7 dicembre 2006, n. 51, *"Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3»*", che sancisce le regole per la vigilanza e il controllo esercitati sui Gestori PEC da Agenzia per l'Italia digitale (ex DigitPA).
- Decreto Legge n. 185/08, convertito nella Legge 28 gennaio 2009, n. 2, che ha introdotto l'obbligo per società, professionisti e Pubbliche Amministrazioni di istituire una versione "virtuale" della sede legale tramite la Posta Elettronica Certificata.

Tra i contenuti della legge n. 2/2009 vengono in rilievo le norme che riguardano:

- le imprese costituite in forma societaria, che devono indicare nella domanda di iscrizione al registro delle imprese il proprio indirizzo di posta elettronica certificata o analogo indirizzo di posta elettronica basato su tecnologie che certifichino data e ora dell'invio e della ricezione delle comunicazioni e l'integrità del contenuto delle stesse, garantendo l'interoperabilità con analoghi sistemi internazionali. L'articolo 16 c. 6 prevede, infatti, che alla tradizionale "sede fisica", venga affiancata una "sede elettronica" presso cui potranno essere recapitati tutti gli atti e i documenti a valore legale.
- per le nuove imprese societarie, l'obbligo è scattato dal 29 novembre 2008 e l'indirizzo PEC va inserito nella domanda di iscrizione nel Registro delle imprese, a cura degli studi notarili che di regola depositano il modello S1 per gli atti costitutivi di società. L'obbligo è scattato immediatamente anche per le Pubbliche Amministrazioni.
- per i professionisti iscritti in albi l'obbligo è stato rinviato di un anno. I professionisti, infatti, entro il 29 novembre 2009 hanno dovuto comunicare ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata. Gli Ordini hanno l'obbligo di curare la pubblicazione in

un elenco riservato, consultabile in via telematica esclusivamente dalle pubbliche amministrazioni, dei dati identificativi degli iscritti con il relativo indirizzo di posta elettronica certificata.

- L'ultima scadenza riguarda le società già iscritte nel Registro delle imprese al 29 novembre 2008, che hanno avuto tempo fino al 30 giugno 2012.
- L'art. 5 del decreto legge 18 ottobre 2012, n. 179 (Ulteriori misure urgenti per la crescita del Paese) in vigore dal 20 ottobre 2012, ha esteso alle imprese individuali l'obbligo di comunicare il proprio indirizzo PEC per l'iscrizione al Registro delle Imprese. Pertanto, dal 20 ottobre 2012, tutte le domande di nuova iscrizione di impresa individuale al Registro Imprese, devono obbligatoriamente contenere la comunicazione dell'indirizzo PEC dell'impresa.
- Le imprese individuali, attive e non soggette a procedure concorsuali, già iscritte nel Registro delle Imprese o all'Albo delle Imprese artigiane prima dell'entrata in vigore del suddetto decreto legge, dovranno provvedere all'iscrizione del proprio indirizzo PEC entro e non oltre il **30 giugno 2013**.
- Infine, vengono citati anche i cittadini, che, mediante opportuna richiesta, potranno ottenere una casella di PEC «*con effetto equivalente alla notificazione per mezzo della posta. Le comunicazioni che transitano per la predetta casella di posta elettronica certificata sono senza oneri*». Le modalità di rilascio e di uso della casella di posta elettronica certificata ai cittadini sono state disciplinate con il successivo DPCM n. 38524/2009.

- Decreto del Presidente del Consiglio dei ministri del 30 marzo 2009 n. 38840 - *"Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici", ora sostituito dal DPCM 22 febbraio 2013, n. 68380*.
- Decreto del Presidente del Consiglio dei ministri del 6 maggio 2009, n. 38524 *"Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini"*.

In sintesi, la normativa prevede:

- le modalità di rilascio della casella di posta elettronica certificata. Tra gli aspetti salienti, viene enunciata la gratuità della stessa qualora questa sia richiesta al Dipartimento per l'innovazione e le tecnologie.
- L'INPS e l'Automobile Club d'Italia, a seguito di un protocollo sottoscritto con il Ministro per la Pubblica Amministrazione e l'Innovazione, concedono una casella di posta elettronica certificata gratuitamente.
- Poste Italiane gestisce invece il servizio "CEC-PAC" ufficiale del Governo italiano, conosciuto anche col nome di "PostaCertificat@" e disponibile sul sito Posta Certificat@ - PostaCertificat@ Mobile - Home Si tratta sì di una casella di Posta Elettronica Certificata gratuita, ma con alcune limitazioni d'uso: una CEC-PAC (Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino), infatti, non consente l'invio o la ricezione di posta se non con caselle PEC della Pubblica Amministrazione. **Viene esclusa quindi la possibilità di comunicazioni fra privati o professionisti o imprese**.

- Decreto del Ministro della Giustizia 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, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24"*.

Con il D.M. in esame sono state adottate le nuove regole tecniche del processo telematico.

La novità di maggiore impatto consiste nell'adozione della posta elettronica certificata standard (PEC) per tutte le trasmissioni da e per il dominio Giustizia.

Il Ministero della giustizia, inoltre, ha messo a disposizione il cosiddetto "Portale dei servizi telematici", al fine di consentire l'accesso ai privati, oltre che agli avvocati non dotati di punto di accesso.

Per l'accesso al portale, infatti, non è richiesto l'impiego di apposite credenziali o sistemi di identificazione e requisiti di legittimazione per poter consultare le informazioni sui servizi telematici del dominio giustizia, le raccolte giurisprudenziali e le informazioni essenziali sullo stato dei procedimenti pendenti, rese disponibili in forma anonima.

La nuova architettura prevede, pertanto, due distinti canali:

- uno per la trasmissione di atti da e verso l'utente esterno (fondato sull'utilizzo della PEC);
- l'altro per l'accesso alle basi dati, anche documentali, attraverso il punto di accesso (PdA) o il portale dei servizi telematici (PST).

È prevista, inoltre, la costituzione del Registro Generale degli Indirizzi Elettronici (**ReGIndE**), gestito dal Ministero della giustizia, contenente i dati identificativi nonché l'indirizzo di PEC dei soggetti abilitati esterni (per la relativa definizione dei soggetti si rimanda all'articolo 2 del D.M. n. 44/2011).

Nessuna modifica, invece, è stata apportata alle specifiche tecniche relative alla creazione della cosiddetta "busta telematica" (contenuto, formati, cifratura e dimensione), contenente gli atti e documenti da trasmettere (in altri termini, la busta continuerà ad essere compilata per mezzo del c.d. redattore atti).

Utilizzando direttamente la propria casella di PEC per effettuare, ad esempio, un deposito, il flusso previsto genererà, sulla casella del depositante, i seguenti messaggi:

1) Ricevuta di Accettazione (RdA), generata dal gestore di PEC del depositante.
2) Ricevuta di Avvenuta Consegna (RdAC) generata dal gestore di PEC del Ministero della giustizia e resa disponibile nella casella di PEC del depositante.
3) Un messaggio di PEC attestante l'esito dei controlli automatici effettuati sulla busta telematica dal gestore dei servizi telematici del Ministero.
4) Un messaggio di PEC attestante l'esito del controllo effettuato da parte dell'operatore di cancelleria sui documenti contenuti nella busta.

- Decreto del Presidente del Consiglio dei ministri del 22 luglio 2011 n. 56784 - *"Comunicazioni con strumenti informatici tra imprese e amministrazioni pubbliche, ai sensi dell'articolo 5-bis del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni".*

In sintesi, la normativa ha previsto che:

- **A decorrere dal 1° luglio 2013, la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avvengono esclusivamente in via telematica.**
- Le amministrazioni centrali provvedono alla completa informatizzazione delle comunicazioni entro il 30 giugno 2013.
- A decorrere dal 1° luglio 2013, le pubbliche amministrazioni non possono accettare o effettuare in forma cartacea le comunicazioni con le imprese.
- A decorrere dalla stessa data, in tutti i casi in cui non è prevista una diversa modalità di comunicazione telematica, le comunicazioni avvengono mediante l'utilizzo della posta elettronica certificata, secondo le disposizioni di cui agli articoli 48 e 65, comma 1, lettera c-bis), del CAD.

- **I casi in cui le istanze e le dichiarazioni presentate alle pubbliche amministrazioni (dalle imprese o da chiunque altro utente) per via telematica devono essere sottoscritte con firma digitale sono, esclusivamente, quelli individuati da appositi decreti ministeriali emanati ai sensi dell'articolo 65, comma 1-bis), del CAD.**

In ottemperanza alle prescrizioni previste dal decreto sono state emanate le Circolari Inail:
- n. 1 del 10 gennaio 2012;
- n. 43 del 14 settembre 2012;
- n. 59 del 31 ottobre 2012;
- n. 61 del 09 novembre 2012;
- nn. 68/69 del 21 dicembre 2012
- n. 19 dell'11 aprile 2013.

- Decreto del Presidente del Consiglio dei ministri del 27 settembre 2012 n. 65329 - *"Regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata, ai sensi dell'articolo 65, comma 1, lettera c-bis), del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005 n. 82 e successive modificazioni"*.
- Il decreto definisce, ai sensi dell'articolo 65, comma 1, lettera c-bis) del CAD, le regole tecniche mediante le quali il gestore della casella di posta elettronica certificata (PEC-ID), tramite la quale possono essere presentate, in via telematica, istanze e dichiarazioni alle pubbliche amministrazioni, deve identificare il titolare della medesima casella. L'identificazione del titolare potrà avvenire mediante la sottoscrizione del modulo di adesione al servizio ed esibizione al gestore, da parte del medesimo, di un valido documento d'identità e del codice fiscale ovvero mediante la sottoscrizione con firma digitale dello stesso modulo ovvero tramite la compilazione del modulo di adesione disponibile in rete, previa identificazione informatica tramite CIE o CNS. L'identificazione per l'accesso al servizio PEC-ID avverrà, invece, tramite Certificato di autenticazione della CNS o della CIE ovvero tramite credenziali di accesso basate su identificativo - utente, parola d'ordine (password) e parola d'ordine temporanea (one time password) generata dal token crittografico rilasciato dal Gestore medesimo e trasmessa anche attraverso sistemi di telefonia mobile.
- Decreto del Ministro della Giustizia 15 ottobre 2012 n. 209 - Regolamento recante: "*Regole tecniche per l'adozione nel processo civile e penale delle tecnologie dell'informazione e comunicazione - modifiche al decreto ministeriale 21 febbraio 2011, n. 44"*.
- Decreto legge 18 ottobre 2012, n. 179 (c.d. "sviluppo bis"), convertito nella legge 17.12.2012, n. 221;

Si segnalano di seguito gli articoli di particolare rilevanza che hanno integrato e modificato il C.A.D.:

Art. 5 - *Posta elettronica certificata (pec) e Indice nazionale degli indirizzi delle imprese e dei professionisti*. La progressiva estensione della Pec alle imprese ed ai professionisti, da effettuarsi entro il 30 giugno 2013, consentirà di utilizzare maggiormente gli strumenti telematici, che gradualmente andranno a sostituire gli invii cartacei. I vantaggi si manifesteranno in termini di tempo e di costi, dal momento che l'utilizzo della Pec equivale a quello di una raccomandata. Il conoscere poi gli indirizzi di posta elettronica di tutti, una volta che divenga pienamente operativo l'Indice nazionale degli indirizzi per imprese e professionisti, consentirà anche alle p.a. di raggiungere celermente la maggior parte dei propri utenti e di risparmiare nell'invio di lettere e raccomandate.

Art. 6 - *Trasmissione telematica di documenti e redazione elettronica di contratti, atti, ecc.* L'art. 6 impone la dematerializzazione dei documenti e l'obbligatorietà di trasmissione per via telematica fra le diverse p.a. Il mancato rispetto della norma determina responsabilità dirigenziale e disciplinare, nonché eventualmente responsabilità per danno erariale, connessa con i costi che si andranno a sostenere per l'utilizzo di carta e posta tradizionale.

Art. 9 - *Documenti informatici e dati di tipo aperto.* L'articolo 9 ha modificato l'art. 54 del Codice dell'amministrazione digitale (Cad), introducendo il principio generale per cui le amministrazioni pubbliche devono rendere disponibili in "formato aperto" i loro dati, consentendo così l'utilizzo e la rielaborazione degli stessi. La maggior parte di questi andrà pubblicata nel sito istituzionale, nell'ambito della sezione "Trasparenza, valutazione e merito" o nelle sezioni specifiche. Anche in questo caso la mancata pubblicazione comporta una precisa responsabilità dirigenziale.

Art. 9-bis - *Acquisto di software da parte delle p.a.* Anche in questo caso si va a modificare il Cad imponendo valutazioni comparative precise tese a privilegiare l'acquisto di software liberi o di soluzioni aperte adeguate che permettano rielaborazioni per gli utilizzi dei dati.

Art. 15 - *Pagamenti elettronici* - L'informatizzazione sempre più spinta dovrà riguardare non solamente i documenti ma anche i sistemi di pagamento. Gli strumenti elettronici semplificheranno i rapporti di cittadini e imprese con la p.a. e si accompagneranno ad un più ampio utilizzo dell'home banking, di carte di credito, carte di debito o di altri strumenti telematici.

- Legge 24.12.2012, n. 228 ("legge di stabilità 2013");
- Decreto Legge 08 aprile 2013 n. 35 *"Disposizioni urgenti per il pagamento dei debiti scaduti della pubblica amministrazione, per il riequilibrio finanziario degli enti territoriali, nonché in materia di versamento di tributi degli enti locali"*;
- Decreto del Ministero dello Sviluppo Economico (MISE) 19 marzo 2013, pubblicato nella G.U. n. 83 del 9 aprile 2013 *"Indice degli indirizzi di posta elettronica certificata delle imprese e dei professionisti*";
- Decreto del Ministero della Giustizia 03 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 penale delle tecnologie dell'informazione e della comunicazione*".

Il Decreto sostituisce il precedente art. 18 del decreto del Ministro della Giustizia 21 febbraio 2011, n. 44.

- Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013, n. 68380.
  Il Decreto sostituisce il DPCM del 30 marzo 2009, n.38840 e detta nuove 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 CAD.
  Le eventuali difformità nella generazione delle firme digitali, delle firme elettroniche qualificate, dei certificati qualificati e delle marche temporali, alle nuove regole tecnologiche di cui al Titolo II, che non ne mettano a rischio la sicurezza, non ne inficiano la validità.
  L'Agenzia per l'Italia Digitale valuta tali difformità e rende note le proprie decisioni sul proprio sito internet.
  Il DPCM prevede, inoltre, che i certificatori accreditati ai sensi dell'art. 29 del CAD, dovranno aggiornare la documentazione ora prevista per lo svolgimento di tale attività entro centoventi giorni dall'entrata in vigore del decreto, ovvero entro il 2 settembre 2013.

3. Decreto Legislativo 7 marzo 2005, n. 82 - C.A.D. (Codice dell'Amministrazione Digitale)

Particolare attenzione, tra le fonti normative in tema di posta elettronica certificata e firma digitale, richiede il decreto legislativo n. 82/2005, il c.d. *Codice dell'amministrazione digitale*, il cui testo più volte integrato e modificato (si ricorda in particolare il decreto legislativo 30 dicembre 2010, n. 235), nella sua versione attuale è stato oggetto, lo scorso anno, di ulteriori interventi ad opera del decreto legge 18 ottobre 2012, n. 179 (il c.d. d.l. "sviluppo bis"), convertito nella legge 17 dicembre 2012, n. 221, nonché, per alcuni versi, dalla legge 24 dicembre 2012, n. 228 ("legge di stabilità 2013").
Di seguito verranno esaminate alcune norme del C.A.D. e la loro applicazione in relazione alle diverse tipologie di utenti:

3.1 Il Cittadino

> Art. 3 bis- CAD - Domicilio digitale del cittadino, articolo inserito dall'articolo 4, comma 1, del D.L. 18 ottobre 2012, n. 179, come modificato dalla Legge 17 dicembre 2012, n. 221.
> art. 62 - CAD - Anagrafe nazionale della popolazione residente-(ANPR), Articolo sostituito dall'articolo 2, comma 1, del D.L. 18 ottobre 2012, n. 179.

Al fine di facilitare la comunicazione tra pubbliche amministrazioni e cittadini, è facoltà di ogni cittadino indicare alla pubblica amministrazione un proprio indirizzo di posta elettronica certificata quale suo domicilio digitale.
L'indirizzo di cui sopra è inserito nell'Anagrafe nazionale della popolazione residente-(ANPR), che prende il posto dell'Indice Nazionale dell'Anagrafe (INA) e dell'Anagrafe della popolazione residente all'estero (AIRE) ed è reso disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi.
Con un prossimo decreto verranno previste forme di aggiornamento e verifica continua dell'effettivo rispetto degli standard di sicurezza ritenuti necessari e saranno, altresì, definite le modalità di comunicazione, variazione e cancellazione del proprio domicilio digitale da parte del cittadino, nonché le modalità di consultazione dell'ANPR da parte dei gestori o esercenti di pubblici servizi ai fini del reperimento del domicilio digitale dei propri utenti. Tale completamento si dovrà realizzare entro il **dicembre del 2014**.
A decorrere dal 1° gennaio 2013, salvo i casi in cui è prevista dalla normativa vigente una diversa modalità di comunicazione o di pubblicazione in via telematica, le amministrazioni pubbliche e i gestori o esercenti di pubblici servizi comunicano con il cittadino esclusivamente tramite il domicilio digitale dallo stesso dichiarato, anche ai sensi dell'articolo 21-bis della legge 7 agosto 1990, n. 241, senza oneri di spedizione a suo carico. Ogni altra forma di comunicazione non può produrre effetti pregiudizievoli per il destinatario.
L'utilizzo di differenti modalità di comunicazione rientra tra i parametri di valutazione della performance dirigenziale ai sensi dell' articolo 11, comma 9, del decreto legislativo 27 ottobre 2009, n. 150.
Le amministrazioni, nelle ipotesi in cui non sono a conoscenza del domicilio digitale del cittadino, predispongono le comunicazioni come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata, da conservare nei propri archivi, ed inviare ai cittadini stessi, per posta ordinaria o raccomandata con avviso di ricevimento, copia

analogica di tali documenti sottoscritti con firma autografa del soggetto responsabile sostituita a mezzo stampa (cfr. art. 3 del D.Lgs. 12 febbraio 1993, n. 39).
Le predette prescrizioni soddisfano a tutti gli effetti di legge gli obblighi di conservazione e di esibizione dei documenti previsti dalla legislazione vigente laddove la copia analogica inviata al cittadino contenga una dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto e conservato presso l'amministrazione in conformità alle regole tecniche previste dall'articolo 71 del CAD.
Le modalità di predisposizione della copia analogica, secondo i criteri sopra delineati, soddisfano pienamente, ai sensi dell'art. 3bis, comma 4quater, le condizioni di certezza ed opponibilità, salvo i casi in cui il documento rappresenti, per propria natura, una certificazione rilasciata dall'amministrazione da utilizzarsi nei rapporti tra privati.
I cittadini che, invece, intendono utilizzare la firma digitale devono registrarsi presso l'autorità di registrazione (RA) del certificatore per l'identificazione e la sottoscrizione del contratto di servizio e fornitura. Inoltre, ogni richiedente ha la possibilità, ai sensi del comma 4 della Deliberazione CNIPA n. 4/2005, di far inserire all'interno del certificato di firma, la specifica qualifica posseduta. Pertanto, al momento della registrazione dovrà consegnare l'eventuale documentazione comprovante il possesso dei titoli.
Le procedure per richiedere il rilascio del certificato (e la fornitura del dispositivo di firma) sono peculiari di ogni certificatore anche se, nella sostanza, prevedono la medesima attività. Dette procedure sono generalmente riportate nel manuale operativo di ogni certificatore ma anche nei rispettivi siti web. Nella scelta del certificatore ogni utente potrà verificare quali servizi aggiuntivi sono forniti dagli stessi (es. certificato di autenticazione e crittografia, casella di posta elettronica certificata), la durata del periodo di validità del certificato ed i costi per il rinnovo.

3.2 L'Impresa ed il Professionista

Art. 6 bis - CAD - Utilizzo della posta elettronica certificata.

La normativa vigente prevede che le camere di commercio e gli ordini e collegi professionali ricevono dai propri iscritti le comunicazioni relative agli indirizzi PEC. Gli indirizzi comunicati da imprese e professionisti vengono inseriti in specifici elenchi a disposizione della pubblica amministrazione.
L'articolo 6 bis del CAD - introdotto dall'art. 5, comma 3, del D.L. 18 ottobre 2012, n. 179, come modificato dalla Legge di conversione 17 dicembre 2012, n. 221 - ha previsto l'istituzione, entro sei mesi dall'entrata in vigore della legge di conversione, dell'**Indice nazionale degli indirizzi PEC delle imprese e dei professionisti (INI-PEC).**
L'INI-PEC, alimentato con le informazioni contenute negli elenchi di indirizzi PEC costituiti presso il registro delle imprese e gli ordini o collegi professionali, favorirà la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica. L'accesso all'INI-PEC sarà consentito alle pubbliche amministrazioni, ai professionisti, alle imprese, ai gestori o esercenti di pubblici servizi ed a tutti i cittadini tramite sito web e senza necessità di autenticazione. L'indice è realizzato in formato aperto, conformemente alle disposizioni di legge.
Il Ministero dello sviluppo economico (MISE), al fine del contenimento dei costi e dell'utilizzo razionale delle risorse, sentita l'Agenzia per l'Italia digitale, si avvale, per la realizzazione e gestione

operativa dell'Indice nazionale, delle strutture informatiche delle Camere di commercio deputate alla gestione del registro imprese e ne definisce le modalità di accesso e di aggiornamento.
Con il decreto del MISE del 19 marzo 2013, pubblicato nella G.U. n. 83 del 9 aprile 2013, sono state puntualmente definite le modalità e le forme con cui gli ordini e i collegi professionali comunicano all'Indice nazionale tutti gli indirizzi PEC relativi ai professionisti di propria competenza e sono previsti gli strumenti telematici resi disponibili dalle Camere di commercio per il tramite delle proprie strutture informatiche al fine di ottimizzare la raccolta e aggiornamento dei medesimi indirizzi.
Per la realizzazione del registro, il decreto ha previsto che entro il 9 giugno dovrà avvenire il trasferimento telematico dei dati già presenti nel Registro delle imprese e di quelli in possesso degli Ordini professionali: nella prima fase, poi, gli aggiornamenti degli indirizzari da parte del Registro imprese e degli Ordini dovranno avvenire ogni 30 giorni. A decorrere da ottobre, invece, le operazioni di aggiornamento avverranno con frequenza giornaliera.
L'indice sarà suddiviso in due sezioni: una per le **imprese** e una per i **professionisti**.
L'INI-Pec sarà consultabile online senza necessità di autenticazione, tramite un portale telematico, ed il suo accesso è consentito alle pubbliche amministrazioni, ai professionisti, alle imprese, ai gestori o esercenti pubblici servizi e a tutti i cittadini .
Sono previsti diversi parametri di ricerca utilizzabili per trovare un'impresa o un professionista: per le imprese, si può utilizzare il parametro del codice fiscale o, in alternativa, della provincia e della ragione sociale/denominazione; per i professionisti la ricerca funzionerà per codice fiscale o per provincia, Ordine e nominativo.

3.3 La trasmissione dei documenti e la cooperazione tra le pubbliche amministrazioni

> Art. 47 - CAD - Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni.
> Art. 50- CAD - Disponibilità dei dati delle pubbliche amministrazioni.
> Art. 57 bis - CAD - Indice degli indirizzi delle pubbliche amministrazioni.
> Art. 58 - CAD - Modalità di fruibilità del dato.
> Art. 63, comma 3 - CAD - Organizzazione e finalità dei servizi in rete.

L'art. 47 del CAD disciplina le modalità di trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni.
Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della **posta elettronica** o in **cooperazione applicativa**; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.
L'inosservanza di questa disposizione, ferma restando l'eventuale responsabilità per danno erariale, comporta, altresì, responsabilità dirigenziale e responsabilità disciplinare.
Ai fini della verifica della provenienza le comunicazioni sono valide se:
a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;
b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;
c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71 del CAD;

d) **ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.**

Le pubbliche amministrazioni devono provvedere ad istituire e pubblicare nell'Indice PA, di cui all'art. 57 bis, almeno una casella di posta elettronica certificata per ciascun registro di protocollo.
Infatti, al fine di assicurare la pubblicità dei riferimenti telematici delle pubbliche amministrazioni e dei gestori dei pubblici servizi è stato istituito l'**I.P.A. - indice degli indirizzi della pubblica amministrazione** e dei gestori di pubblici servizi, nel quale sono indicati gli indirizzi di posta elettronica certificata da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi ed i privati.
La realizzazione e la gestione dell'indice sono affidate all'Agenzia per l'Italia Digitale, che può utilizzare elenchi e repertori già formati dalle amministrazioni pubbliche.
Le amministrazioni devono aggiornare gli indirizzi e i contenuti dell'indice tempestivamente e comunque con cadenza almeno semestrale secondo le indicazioni dell'Agenzia. La mancata comunicazione degli elementi necessari al completamento dell'indice e del loro aggiornamento è valutata ai fini della responsabilità dirigenziale e dell'attribuzione della retribuzione di risultato ai dirigenti responsabili.
La pubbliche amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.
Il Decreto Legislativo 14 marzo 2013, n. 33, recentemente, ha riordinato la disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.
La normativa in questione non ha apportato particolari innovazioni nella materia oggetto della presente trattazione in quanto la disciplina dettata dal CAD risulta essere sull'argomento particolarmente progredita.
Infatti, in merito alla disponibilità dei dati delle pubbliche amministrazioni, l'art. 50 del "Codice", prevede già che questi debbano essere resi disponibili ed accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, da parte delle altre pubbliche amministrazioni e dai privati. Qualunque dato trattato da una P.A., pertanto, salvo casi specifici e nel rispetto della normativa in materia di privacy, deve essere reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato è reso necessario per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente. A tal fine il successivo art. 58, secondo comma, prescrive che le amministrazioni titolari di banche dati accessibili per via telematica debbano predisporre apposite convenzioni aperte all'adesione di tutte le amministrazioni interessate volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti, senza oneri a loro carico.
Le stesse pubbliche amministrazioni devono, infine, ai sensi dell'art. 63, comma 3 del CAD, collaborare fattivamente per integrare i procedimenti di rispettiva competenza al fine di agevolare gli adempimenti di cittadini ed imprese e rendere più efficienti i procedimenti che interessano più amministrazioni, attraverso **idonei sistemi di cooperazione** (v. supra par.1.5, ultima parte).

3.4 La pubblica amministrazione

Art. 38 D.P.R. 445/2000
Artt. 5bis, 6, 17, 48, 54, 63, 64 e 65 - CAD
D.P.C.M. 22 luglio 2011, n. 56784
Art. 1 commi 29/30 legge 190/2012 - legge anticorruzione
Decreto MISE 19 marzo 2013

- Organizzazione
Ai sensi dell'art. 17 del CAD, le pubbliche amministrazioni centrali, con l'emanazione di singoli provvedimenti, garantiscono l'attuazione delle linee strategiche per la riorganizzazione e digitalizzazione dell'amministrazione nei termini definiti dal Governo. A tale fine individuano un unico ufficio dirigenziale generale responsabile del coordinamento funzionale. Al predetto ufficio afferiscono, in particolare, i compiti relativi alla **pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale e mandato informatico, e delle norme in materia di accessibilità e fruibilità.**

La P.A., oltre ad occuparsi dei processi di diffusione interna dei predetti concetti, deve, altresì, provvedere, a tenore dell'art. 54 del CAD, a rendere fruibili ed accessibili dall'esterno una serie di dati pubblici:

- l'organigramma, l'articolazione degli uffici, le attribuzioni e l'organizzazione di ciascun ufficio anche di livello dirigenziale non generale i nomi dei dirigenti responsabili dei singoli uffici, nonché il settore dell'ordinamento giuridico riferibile all'attività da essi svolta, corredati dai documenti anche normativi di riferimento;
- l'elenco delle tipologie di procedimento svolte da ciascun ufficio di livello dirigenziale non generale, il termine per la conclusione di ciascun procedimento ed ogni altro termine procedimentale, il nome del responsabile e l'unità organizzativa responsabile dell'istruttoria e di ogni altro adempimento procedimentale, nonché dell'adozione del provvedimento finale, come individuati ai sensi degli articoli 2, 4 e 5 della legge 7 agosto 1990, n. 241;
- le scadenze e le modalità di adempimento dei procedimenti individuati ai sensi degli articoli 2 e 4 della legge 7 agosto 1990, n. 241;
- **l'elenco completo delle caselle di posta elettronica istituzionali attive, specificando anche se si tratta di una casella di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68;**
- le pubblicazioni di cui all'articolo 26 della legge 7 agosto 1990, n. 241, nonché i messaggi di informazione e di comunicazione previsti dalla legge 7 giugno 2000, n. 150;
- l'elenco di tutti i bandi di gara;
- l'elenco dei servizi forniti in rete già disponibili e dei servizi di futura attivazione, indicando i tempi previsti per l'attivazione medesima.
- i bandi di concorso.

Le pubbliche amministrazioni centrali devono comunicare, in via telematica, al Dipartimento della funzione pubblica, che a sua volta provvederà a pubblicarli sul proprio sito istituzionale, i dati di cui alle lettere b), c) , g) e h). La mancata comunicazione o aggiornamento dei dati è comunque rilevante ai fini della misurazione e valutazione della performance individuale dei dirigenti.

Le amministrazioni pubbliche e i gestori di servizi pubblici sono tenuti, altresì, a pubblicare nei propri siti un indirizzo istituzionale di posta elettronica certificata a cui il cittadino possa rivolgersi per qualsiasi richiesta. Le amministrazioni devono altresì assicurare un servizio che renda noti al pubblico i tempi di risposta.

Le amministrazioni pubbliche che già dispongono di propri siti devono pubblicare il registro dei processi automatizzati rivolti al pubblico. Tali processi devono essere dotati di appositi strumenti per la verifica a distanza da parte del cittadino dell'avanzamento delle pratiche che lo riguardano.

I dati pubblici contenuti nei siti delle pubbliche amministrazioni sono fruibili in rete gratuitamente e senza necessità di identificazione informatica.

A tal fine, le pubbliche amministrazioni garantiscono che le informazioni contenute sui siti siano accessibili, conformi e corrispondenti alle informazioni contenute nei provvedimenti amministrativi originali dei quali si fornisce comunicazione tramite il sito.

La pubblicazione telematica produce effetti di pubblicità legale nei casi e nei modi **espressamente previsti** dall'ordinamento.

Le pubbliche amministrazioni centrali, ai sensi dell'art. 63 del CAD, devono individuare le modalità di erogazione dei servizi in rete in base a criteri di valutazione di efficacia, economicità ed utilità e nel rispetto dei principi di eguaglianza e non discriminazione, tenendo comunque presenti le dimensioni dell'utenza, la frequenza dell'uso e l'eventuale destinazione all'utilizzazione da parte di categorie in situazioni di disagio.

Le PP.AA., inoltre, devono progettare e realizzare i servizi in rete mirando alla migliore soddisfazione delle esigenze degli utenti, in particolare garantendo la completezza del procedimento, la certificazione dell'esito e l'accertamento del grado di soddisfazione dell'utente. A tal fine, sono tenuti ad adottare strumenti idonei alla rilevazione immediata, continua e sicura del giudizio degli utenti.

A partire dal **1º gennaio 2014**, allo scopo di incentivare e favorire il processo di informatizzazione e di potenziare ed estendere i servizi telematici, le pubbliche amministrazioni - nonché le società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) - utilizzano **esclusivamente** i canali e i servizi telematici, ivi inclusa la posta elettronica certificata, per l'erogazione - anche a mezzo di intermediari abilitati- dei propri servizi, ovvero per la presentazione da parte degli interessati di:

- denunce;
- istanze;
- atti e garanzie fideiussorie;
- l'esecuzione di versamenti fiscali, contributivi, previdenziali, assistenziali e assicurativi;
- richiesta di attestazioni e certificazioni.

A partire dal 1º gennaio 2014 i soggetti di sui sopra dovranno utilizzare **esclusivamente** servizi telematici o la posta elettronica certificata anche per gli atti, le comunicazioni o i servizi dagli stessi resi.

I medesimi soggetti, almeno sessanta giorni prima della data della loro entrata in vigore, pubblicano nel sito web istituzionale l'elenco dei provvedimenti adottati secondo criteri telematici, nonché termini e modalità di utilizzo dei servizi e dei canali telematici e della posta elettronica certificata.

- Documentazione amministrativa

Ai sensi dell'art. 38 del Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 - *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa* - tutte le istanze e le dichiarazioni da presentare alla pubblica amministrazione o ai gestori o esercenti di pubblici servizi possono essere inviate anche per fax e via telematica.

I documenti trasmessi da chiunque ad una pubblica amministrazione con qualsiasi mezzo telematico o informatico, idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale.

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.

Le istanze e le dichiarazioni inviate per via telematica, ivi comprese le domande per la partecipazione a selezioni e concorsi per l'assunzione, a qualsiasi titolo, in tutte le pubbliche amministrazioni, o per l'iscrizione in albi, registri o elenchi tenuti presso le pubbliche amministrazioni, sono valide se effettuate secondo quanto previsto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82

Il primo comma dell'articolo sopra citato dispone che le istanze e le dichiarazioni presentate per via telematica 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, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;

c) ovvero quando l'autore è identificato dal sistema informatico con i diversi strumenti di cui all'articolo 64, comma 2, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente nonché quando le istanze e le dichiarazioni sono inviate con le modalità di cui all'articolo 38, comma 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

> Il comma 3 dell'articolo 38, sopra richiamato, dispone, tra l'altro, che la copia dell'istanza sottoscritta dall'interessato e la copia del documento di identità possono essere inviate per via telematica; in assenza di ulteriori specificazioni, deve ritenersi valido anche l'invio a mezzo di posta elettronica non certificata.

c-bis) ovvero se trasmesse dall'autore mediante la 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'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce dichiarazione vincolante ai sensi dell'articolo 6, comma 1, secondo periodo. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario.

Il comma 1-bis dello stesso articolo 65 prevede che, con decreto del Ministro per la pubblica amministrazione e l'innovazione e del Ministro per la semplificazione normativa, possono essere individuati i casi in cui è comunque richiesta la sottoscrizione del documento mediante firma digitale.

- Trasmissione telematica

Ai sensi dell'art. 48 del CAD, la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene, ormai in massima parte, mediante la posta elettronica certificata.

La trasmissione del documento informatico per via telematica, effettuata tramite PEC, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.

Pertanto, la data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso con le predette modalità, 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.

L'art. 6 CAD, ha chiarito che per le comunicazioni di cui all'articolo 48, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni devono utilizzare la posta elettronica certificata. La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano.

Il mancato avvio del procedimento da parte del titolare dell'ufficio competente a seguito di istanza o dichiarazione inviate per via telematica, comporta responsabilità dirigenziale e responsabilità disciplinare dello stesso.

La recente legge 6 novembre 2012 n. 190 - *Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione* - è intervenuta nuovamente sulla materia per stabilire che ogni amministrazione pubblica deve rendere noto, tramite il proprio sito web istituzionale, almeno un indirizzo di **posta elettronica certificata** cui il cittadino possa rivolgersi per trasmettere istanze ai sensi dell'articolo 38 del D.P.R. n. 445/2000 e ricevere informazioni circa i provvedimenti e i procedimenti amministrativi che lo riguardano.

Le amministrazioni, nel rispetto della disciplina del diritto di accesso ai documenti amministrativi, hanno l'obbligo di rendere accessibili in ogni momento agli interessati, tramite strumenti di **identificazione informatica** di cui all'articolo 65, comma 1, del CAD, le informazioni relative ai provvedimenti e ai procedimenti amministrativi che li riguardano, ivi comprese quelle relative allo stato della procedura, ai relativi tempi e allo specifico ufficio competente in ogni singola fase.

Per quanto concerne nello specifico i **rapporti tra le imprese e le amministrazioni pubblich**e, il D.P.C.M. 22 luglio 2011 n. 56784, ha stabilito che, a decorrere dal **1° luglio 2013**, la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, devono avvenire **esclusivamente** in via telematica, tramite un "Portale" dedicato.

A tal fine le amministrazioni centrali provvedono alla completa informatizzazione delle comunicazioni entro il 30 giugno 2013.

Ferme restando le procedure informatizzate già attive, le comunicazioni, fino alla data del 1° luglio 2013, possono essere effettuate tramite la posta elettronica certificata di cui all'articolo 65, comma 1, lettera c-bis) del CAD.

Almeno ogni sei mesi dovrà essere pubblicato sui siti istituzionali di ciascuna amministrazione l'elenco dei procedimenti amministrativi relativamente ai quali le comunicazioni di cui sopra sono svolte esclusivamente in via telematica, con l'indicazione della data di decorrenza, comunque non superiore a sessanta giorni.

I programmi e gli elenchi delle procedure già informatizzate sono comunicati all'Agenzia per l'Italia Digitale, ex DigitPA, per la verifica dell'attuazione di quanto previsto dal Codice dell'amministrazione digitale.

A decorrere dal 1° luglio 2013, le pubbliche amministrazioni non possono, nei rapporti con le imprese, accettare o effettuare in forma cartacea le comunicazioni di cui all'articolo 5-bis, comma 1, del CAD, ovvero, presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti.

A decorrere dalla stessa data, in tutti i casi in cui non é prevista una diversa modalità di comunicazione telematica, le comunicazioni devono avvenire esclusivamente mediante l'utilizzo della posta elettronica certificata, secondo le disposizioni di cui agli articoli 48 e 65, comma 1, lettera c-bis), del CAD.

L'inosservanza delle scadenze sopra evidenziate, nonché più in generale, l'inosservanza o la mancata attuazione delle disposizioni del "Codice", costituisce, ex art. 12, comma 1ter, del CAD, ipotesi di responsabilità dirigenziale ai sensi dell'articolo 21, comma 1, del decreto legislativo 30 marzo 2001, n. 165. Di contro, l'attuazione e l'osservanza delle predette disposizioni e di tutte le disposizioni del "Codice" sono rilevanti, ai sensi medesimo articolo del CAD, ai fini della misurazione e valutazione della performance organizzativa e di quella individuale dei dirigenti.

Si precisa, inoltre, che la consultazione degli indirizzi di posta elettronica certificata, e l'estrazione di elenchi dei suddetti indirizzi, da parte delle pubbliche amministrazioni è effettuata sulla base delle regole tecniche emanate dall'Agenzia per l'Italia Digitale, sentito il Garante per la protezione dei dati personali.

In particolare, per la consultazione dell'Indice nazionale degli indirizzi PEC delle imprese e dei professionisti (INI-PEC), l'art. 6 del decreto 19 marzo 2013 del MISE, ha previsto che al fine di facilitare l'utilizzo dei dati relativi agli indirizzi PEC, possono essere resi disponibili da InfoCamere alle Pubbliche amministrazioni, ai gestori dei servizi pubblici e agli operatori economici interessati, nel rispetto di quanto disposto in materia di tutela delle privacy, servizi evoluti di accesso, consultazione ed estrazione da regolamentarsi tramite apposite convenzioni.

Per quanto riguarda, invece, le modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni, l'art. 64 del "Codice" stabilisce che la carta d'identità elettronica e la carta nazionale dei servizi, previa necessaria identificazione informatica, costituiscono gli strumenti principali, ma non esclusivi, per l'accesso ai servizi erogati in rete. Infatti, le PP.AA. possono, altresì, consentire l'accesso ai servizi in rete che richiedono l'identificazione informatica, anche con strumenti diversi purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio.

II - PARTE SPECIALE

4. Appalti Pubblici

Con l'art. 20 del decreto legge 09 febbraio 2012, n. 5 convertito, con modificazioni nella legge n. 35 del 04 aprile 2012 *"disposizioni urgenti in materia si semplificazioni e sviluppo"* sono state apportate modifiche al decreto legislativo 12 aprile 2006, n. 163 ed al decreto legislativo 7 marzo 2005, n. 82.
Nel decreto legislativo 12 aprile 2006, n. 163, viene inserito l'art. 6-bis con il quale si attribuiscono particolari competenze alla Banca Dati Nazionale dei Contratti Pubblici.
Dal **1 gennaio 2013** la documentazione comprovante il possesso dei requisiti di carattere generale, tecnico-organizzativo ed economico-finanziario per la partecipazione alle procedure disciplinate dal Codice dei Contratti Pubblici è acquisita, pertanto, presso la Banca Dati Nazionale dei Contratti Pubblici, istituita presso l'Autorità per la vigilanza sui contratti pubblici di lavori dall'art. 62-bis del decreto legislativo 7 marzo 2005, n. 82.

Con la **deliberazione n. 111 del 20 dicembre 2012**, l'Autorità, oltre a prevedere una gradualità per l'entrata a regime della nuova procedura, ha fornito puntuali istruzioni con le quali le stazioni appaltanti e gli enti aggiudicatori devono verificare il possesso dei predetti requisiti degli operatori economici.
A tal fine i soggetti pubblici e privati che detengono i dati e la documentazione relativi ai requisiti suindicati sono tenuti a metterli a disposizione dell'Autorità entro i termini e secondo le modalità previste dalla stessa Autorità.
Con le medesime modalità gli operatori economici sono tenuti altresì ad integrare i dati contenuti nella Banca Dati Nazionale dei Contratti Pubblici.
L'Autorità, per perseguire le finalità di semplificazione delle procedure di affidamento dei contratti pubblici, istituisce, quindi, un sistema per la verifica online dei requisiti per la partecipazione alle procedure di affidamento, denominato "AVC$_{PASS}$" (Authority Virtual Company Passport).
AVC$_{PASS}$ consente alle stazioni appaltanti/enti aggiudicatori, attraverso un'interfaccia web, l'acquisizione della documentazione comprovante il possesso dei requisiti di partecipazione alle procedure di affidamento. Secondo quanto disposto dagli art. 2 e 4 della Deliberazione, la stazione appaltante/ente aggiudicatore, acquisito il CIG, specifica in AVC$_{PASS}$ i requisiti speciali di partecipazione alla procedura e i relativi documenti di comprova, **indicando contestualmente i soggetti abilitati a compiere le verifiche e, quindi, dotati di apposita casella PEC, essendo questo un imprescindibile presupposto per operare nel sistema.**
L'operatore economico, effettuata la registrazione al servizio AVC$_{PASS}$ e individuata la procedura di affidamento cui intende partecipare, ottiene dal sistema un "PASSOE" da inserire nella busta contenente la documentazione amministrativa. Inoltre, gli operatori economici, tramite un'area dedicata, inseriscono a sistema i documenti relativi alla dimostrazione del possesso dei requisiti di capacità economico finanziaria e tecnico professionale che sono nella loro esclusiva disponibilità e, pertanto, non reperibili presso Enti certificatori. L'operatore economico può utilizzare tali documenti, purché in corso di validità, per tutte le successive procedure di affidamento alle quali partecipi.
Al fine di garantire che le richieste di verifica dei requisiti interessino unicamente i partecipanti alla specifica procedura, prima di poter accedere alla comprova dei requisiti, il soggetto

abilitato alla verifica dalla stazione appaltante, integra o conferma l'elenco degli operatori economici partecipanti alla procedura di affidamento. Nel caso in cui siano presenti operatori economici che non si sono registrati in AVC$_{PASS}$, la stazione appaltante li invita a provvedere in un termine congruo rispetto all'avvio dell'attività di verifica. È appena il caso di rilevare che, pur non rappresentando la registrazione al sistema una condizione di partecipazione, tuttavia essa costituisce, per espressa previsione del legislatore, la modalità esclusiva di verifica dei requisiti. A fronte della mancata registrazione di un operatore economico sottoposto a verifica, la stazione appaltante pertanto non sarà in condizione di appurare la veridicità delle dichiarazioni presentate.
Ai fini delle verifiche, la stazione appaltante, attraverso il soggetto abilitato, trasmette tramite AVC$_{PASS}$ la richiesta dei documenti a comprova dei requisiti per gli operatori economici selezionati; successivamente l'Autorità avvia presso gli Enti certificatori le richieste dei documenti, mettendoli a disposizione del soggetto abilitato non appena disponibili.
Entro il termine di 60 giorni dall'aggiudicazione definitiva, il Responsabile del Procedimento deve trasferire definitivamente sui propri sistemi, mediante l'apposita funzionalità, i fascicoli di gara e i documenti in essi contenuti. Trascorsi 4 giorni dalla scadenza del termine, l'Autorità procede ad inviare la documentazione via PEC alla stazione appaltante/ente aggiudicatore. Tale invio costituisce consegna ufficiale della documentazione di gara.
Appare utile evidenziare che eventuali richieste di accesso agli atti devono essere rivolte esclusivamente alla stazione appaltante/ente aggiudicatore, per motivi di carattere tecnico, giuridico e di economia gestionale. In primo luogo, molti dei documenti vengono acquisiti da AVC$_{PASS}$ per la consultazione dei soli soggetti abilitati. Inoltre, la stazione appaltate procedente è l'unico soggetto legittimato a compiere l'attività di acquisizione delle istanze di accesso e di valutazione e contemperamento di tutti gli interessi sottesi.
L'art. 3 individua le modalità di comunicazione che devono adottare i soggetti abilitati dalla stazione appaltante/ente aggiudicatore (RUP, Presidente di Commissione e Commissari di gara) e l'operatore economico (amministratore/legale rappresentante), che in relazione alla singola gara interagiscono attraverso il sistema AVC$_{PASS}$. **Viene, in particolare, prescritto che, oltre al responsabile del procedimento, sia dotato di casella di PEC anche ciascuno dei soggetti sopraindicati, laddove chiamato dalla stazione appaltante ad operare tramite il sistema, e che i documenti inseriti dagli operatori economici siano firmati digitalmente.**
Al fine di consentire agli operatori economici e alle stazioni appaltanti/enti aggiudicatori di adeguarsi gradualmente alle nuove modalità di verifica dei requisiti, l'obbligo di procedere alla verifica stessa attraverso l'utilizzo del sistema AVC$_{PASS}$, ai sensi dell'art. 9, decorre secondo le seguenti scadenze temporali:

a) Dal **1° gennaio 2013** per gli appalti di lavori in procedura aperta nel settore ordinario, di importo a base d'asta pari o superiore a € 20.000.000;
b) Dal **1°marzo 2013** per tutti gli appalti di importo a base d'asta pari o superiore a € 40.000,00, con esclusione di quelli svolti attraverso procedure interamente gestite con sistemi telematici, sistemi dinamici di acquisizione o mediante ricorso al mercato elettronico, nonché quelli relativi ai settori speciali.

In via transitoria, fino al 30 giugno 2013, le stazioni appaltanti/enti aggiudicatori per tali appalti possono continuare a verificare il possesso dei requisiti degli operatori economici secondo le previgenti modalità.

A far data dal **1° luglio 2013** gli appalti di importo a base d'asta pari o superiore a € 40.000,00 di cui ai commi a) e b) entrano in regime di obbligatorietà.

c) Dal **1° ottobre 2013** per gli appalti di importo a base d'asta pari o superiore a € 40.000,00 svolti attraverso procedure interamente gestite con sistemi telematici, sistemi dinamici di acquisizione ed il ricorso al mercato elettronico, nonché per i settori speciali.

In via transitoria, fino al 31 dicembre 2013, le stazioni appaltanti/enti aggiudicatori per tali appalti possono continuare a verificare il possesso dei requisiti degli operatori economici secondo le previgenti modalità.

A far data dal **1° gennaio 2014** il regime di obbligatorietà è esteso anche a quest'ultimi appalti.
Il Presidente dell'Inail, con Determina del **1° marzo 2013,** n. 62, ha approvato lo schema di convenzione per la cooperazione applicativa tra l'Autorità per la Vigilanza sui Contratti Lavori, Servizi e Forniture e l'Inail.
La Convenzione si prefigge di regolare lo scambio delle informazioni di cui le parti sono titolari e che si rendono necessarie per rispondere a specifici compiti loro assegnati dalla normativa vigente, attraverso l'interoperabilità e la cooperazione applicativa dei sistemi informatici e dei flussi informativi.
Con la medesima convenzione è regolato, altresì, lo scambio di informazioni, nel rispetto degli obiettivi del piano di *e-government* volti ad assicurare la condivisione, l'integrazione e la circolarità del patrimonio informativo e dei dati della pubblica amministrazione, con la finalità di favorire la riduzione degli oneri amministrativi derivanti dagli obblighi informativi.
L'Autorità ha già individuato i dati e le informazioni oggetto di condivisione di proprio interesse nell'art. 5, comma 1, lett. f), della citata deliberazione n. 111 del 20 dicembre 2012.

5. La procedura di sospensione della riscossione ex art. 1, commi 537/544 legge 24 dicembre 2012, n. 228 (Legge di stabilità)

L'articolo 1 (commi da 537 a 544) della legge di stabilità 2013 ha introdotto nel nostro ordinamento la possibilità di sospendere la riscossione ad iniziativa del debitore che presenti all'agente della riscossione, entro 90 giorni dalla notifica di un atto, una dichiarazione con la quale venga documentato che gli atti emessi dall'ente creditore prima della formazione del ruolo, ovvero la successiva cartella di pagamento o l'avviso per i quali si procede, sono stati interessati da prescrizione o decadenza, da provvedimento di sgravio, da sospensione amministrativa o giudiziale, da sentenza che ha annullato in tutto o in parte la pretesa dell'ente creditore, dal pagamento già effettuato o da qualsiasi altra causa di non esigibilità del credito.
Pertanto, dal 1° gennaio 2013 i «concessionari per la riscossione», devono sospendere immediatamente ogni iniziativa finalizzata alla riscossione delle somme iscritte a ruolo o affidate, su presentazione di una dichiarazione da parte del debitore che fa valere profili di illegittimità.
Entro novanta giorni dalla notifica del primo atto di riscossione utile o di un atto della procedura cautelare o esecutiva eventualmente intrapresa dal concessionario, il contribuente presenta al concessionario per la riscossione una dichiarazione anche con **modalità telematiche**, con la quale venga documentato che gli atti emessi dall'ente creditore prima della formazione del

ruolo, ovvero la successiva cartella di pagamento o l'avviso per i quali si procede, sono stati interessati:

a) da prescrizione o decadenza del diritto di credito sotteso, intervenuta in data antecedente a quella in cui il ruolo è reso esecutivo;
b) da un provvedimento di sgravio emesso dall'ente creditore;
c) da una sospensione amministrativa comunque concessa dall'ente creditore;
d) da una sospensione giudiziale, oppure da una sentenza che abbia annullato in tutto o in parte la pretesa dell'ente creditore, emesse in un giudizio al quale il concessionario per la riscossione non ha preso parte;
e) da un pagamento effettuato, riconducibile al ruolo in oggetto, in data antecedente alla formazione del ruolo stesso, in favore dell'ente creditore;
f) da qualsiasi altra causa di non esigibilità del credito sotteso.

Entro dieci giorni successivi alla data di presentazione della dichiarazione del contribuente, il concessionario per la riscossione trasmette all'ente creditore la dichiarazione e la documentazione allegata.

Decorsi ulteriori sessanta giorni, quindi complessivamente settanta dalla data di presentazione della dichiarazione, l'ente creditore e' tenuto, con propria comunicazione inviata al debitore a mezzo raccomandata con ricevuta di ritorno o a mezzo posta elettronica certificata, a confermare allo stesso la correttezza della documentazione prodotta, provvedendo, in pari tempo, a trasmettere in via telematica, al concessionario della riscossione il conseguente provvedimento di sospensione o sgravio, ovvero ad avvertire il debitore dell'inidoneità di tale documentazione a mantenere sospesa la riscossione, dandone, anche in questo caso, immediata notizia al concessionario della riscossione per la ripresa dell'attività di recupero del credito iscritto a ruolo.
Laddove l'ente creditore non adempia al predetto obbligo, trascorso inutilmente il termine di duecentoventi giorni dalla data di presentazione della dichiarazione del debitore al concessionario della riscossione, le partite relative agli atti espressamente indicate dal debitore sono annullate di diritto e quest'ultimo è considerato automaticamente discaricato dei relativi ruoli. Contestualmente sono eliminati dalle scritture patrimoniali dell'ente creditore i corrispondenti importi.
Oltre alla responsabilità penale, nel caso in cui il contribuente, produca documentazione falsa, si applica la sanzione amministrativa dal 100 al 200 per cento dell'ammontare delle somme dovute, con un importo minimo di 258 euro.
I concessionari per la riscossione sono tenuti a fornire agli enti creditori il massimo supporto per l'automazione delle fasi di trasmissione di provvedimenti di annullamento o sospensione dei carichi iscritti a ruolo.
Le predette disposizioni si applicano anche alle dichiarazioni presentate al concessionario della riscossione prima della data di entrata in vigore della legge di stabilità (1° gennaio 2013). L'ente creditore, in tali ipotesi, invia la comunicazione e provvede agli adempimenti previsti entro 90 giorni dalla data di pubblicazione della legge di stabilità (29 dicembre 2012); in mancanza, trascorso inutilmente il termine di 220 giorni dalla stessa data, le partite relative agli atti espressamente indicate dal debitore sono annullate di diritto ed il concessionario della riscossione è considerato automaticamente discaricato dei relativi ruoli. Contestualmente sono eliminati dalle scritture patrimoniali dell'ente creditore i corrispondenti importi.

In tutti i casi di riscossione coattiva di debiti fino a mille euro, ai sensi del decreto del Presidente della Repubblica 29 settembre 1973, n. 602, intrapresa successivamente al 1° gennaio 2013, salvo il caso in cui l'ente creditore abbia notificato al debitore la comunicazione di inidoneità della documentazione, non si procede alle azioni cautelari ed esecutive prima del decorso di centoventi giorni dall'invio, mediante posta ordinaria, di una comunicazione contenente il dettaglio delle iscrizioni a ruolo.

Successivamente all'entrata in vigore della normativa, l'Agenzia delle Entrate - Direzione accertamento - con la nota del **16 gennaio 2013** diretta agli uffici periferici ed Equitalia ha emanato puntuali direttive sulla nuova procedura per la sospensione legale della riscossione.
L'Agenzia ha chiarito che la procedura per la richiesta di sospensione, da parte del debitore da presentarsi entro 90 giorni dalla notifica dell'atto, è esperibile non solo per le cartelle di pagamento ma anche per altri atti (come gli avvisi di accertamento esecutivi).
L'Agenzia evidenzia, altresì, come la nuova sospensione legale è di portata più ampia rispetto a quella di 180 giorni relativa all'esecuzione forzata prevista dall'articolo 29 comma 1 lett. b) del Dl 78/2010. Quest'ultima, infatti, opera con esclusivo riferimento agli atti esecutivi, facendo espressamente salva ogni iniziativa cautelare o conservativa e senza coinvolgere l'ente creditore.
La nuova procedura, invece, sospende immediatamente dalla data di presentazione dell'istanza del contribuente, ogni attività dell'Agente della riscossione, fino a quando le ragioni indicate nella dichiarazione prodotta non siano ritenute inidonee.

6. La procedura di "certificazione dei crediti"

> Articolo 9, commi 3-bis e 3-ter del decreto legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2 e successive modificazioni.
> D.M. MEF 22 maggio 2012 n. 61398 e successive modificazioni.
> Circolare MEF n. 35 del 27 novembre 2012.
> Art. 7, decreto legge 8 aprile 2013 n. 35.

Il 22 maggio 2012 il Governo ha emanato le nuove misure volte a disciplinare i rapporti di credito e debito tra la Pubblica Amministrazione e le imprese fornitrici.
In particolare, rientra fra tali misure, il "decreto certificazione", avente ad oggetto la certificazione dei crediti scaduti nei confronti delle amministrazioni centrali (inclusi gli enti pubblici nazionali).
A seguito delle modifiche introdotte dal decreto legge 7 maggio 2012, n. 52, convertito con modificazioni dalla L. 6 luglio 2012, n. 94 sono stati emanati i decreti ministeriali di recepimento di tali modifiche:

- il D.M. 24 settembre 2012 di modifica del decreto 22 maggio 2012;
- il D.M. 19 ottobre 2012 avente ad oggetto le modalità con le quali i crediti non prescritti certi liquidi ed esigibili maturati nei confronti dello Stato e degli enti pubblici nazionali per somministrazioni, forniture e appalti, possono essere compensati con le somme dovute a seguito di iscrizione a ruolo ai sensi dell'articolo 28-quater del decreto del Presidente della Repubblica 29 settembre 1973, n. 602.

Per favorire lo smobilizzo dei crediti vantati dalle imprese nei confronti della P.A., i "decreti

certificazione" attuano l'obbligo per lo Stato, gli enti pubblici nazionali, le regioni, gli enti locali e gli enti del Servizio Sanitario Nazionale di certificare, su istanza del creditore, gli eventuali crediti relativi a somme dovute per somministrazioni, forniture e appalti (il credito deve riferirsi ad un contratto avente ad oggetto somministrazioni, forniture ed appalti, secondo le definizioni recate dal decreto legislativo 12 aprile 2006, n. 163).
L'istanza di certificazione può essere presentata da chiunque, società, impresa individuale o persona fisica, vanti un credito non prescritto, certo, liquido ed esigibile, scaturente da un contratto avente ad oggetto somministrazioni, forniture ed appalti nei confronti di una P.A.

- Ai fini dell'ottenimento della certificazione il credito deve essere, quindi, certo, liquido ed esigibile:
  a) il credito è da considerarsi certo quando è determinato nel suo contenuto dal relativo atto negoziale, perfezionatosi, nel caso di specie, secondo le forme e le procedure prescritte dalla vigenti disposizioni contabili. Ai fini della certificazione, è da ritenersi sussistente il requisito della certezza solo qualora il credito sia afferente ad una obbligazione giuridicamente perfezionata per la quale sia stato assunto il relativo impegno di spesa, registrato sulle scritture contabili ovvero, per gli enti del Servizio Sanitario Nazionale, siano state effettuate le relative registrazioni contabili. Pertanto, in assenza di contratto perfezionato o di impegno di spesa, regolarmente registrato sulle scritture contabili ovvero, per gli enti del Servizio Sanitario Nazionale, delle necessarie registrazioni contabili, gli enti non potranno certificare il credito, riferibile esclusivamente alla sfera giuridica del soggetto che ha ordinato la somministrazione, la fornitura o l'appalto al di fuori delle prescritte procedure giuscontabili;
  b) il requisito della liquidità, soddisfatto dalla quantificazione dell'esatto ammontare del credito, è da ricondursi agli elementi del titolo giuridico;
  c) l'esigibilità, da valutarsi al momento del riscontro da parte delle amministrazioni, sta ad indicare l'assenza di fattori impeditivi del pagamento del credito, quali l'eccezione di inadempimento, l'esistenza di un termine o di una condizione sospensiva.

Fermo restando il requisito di non prescrizione del credito, le norme non indicano alcun termine entro il quale inoltrare le istanze di certificazione.
Non sono in ogni caso certificabili le somme relative a debiti fuori bilancio delle amministrazioni.
L'istanza di certificazione può essere presentata per i crediti vantati nei confronti di
- amministrazioni statali, centrali e periferiche;
- enti pubblici non economici;
- regioni e province autonome;
- enti locali;
- enti del Servizio Sanitario Nazionale.

La certificazione non può essere rilasciata, a pena di nullità, dai seguenti enti:
- enti locali commissariati;
- enti del Servizio Sanitario Nazionale delle regioni sottoposte a piano di rientro dai disavanzi sanitari, ovvero a programmi operativi di prosecuzione degli stessi, se nell'ambito di detti piani o di detti programmi sono previste operazioni relative al debito.

Non è possibile richiedere la certificazione per i crediti vantati nei confronti di:
- organi costituzionali e a rilevanza costituzionale;
- camere di commercio, industria, artigianato e agricoltura e loro associazioni;

- enti pubblici economici;
- enti ed organismi di diritto privato;
- società a partecipazione pubblica.

6.1 La procedura ordinaria e la procedura telematica

Il procedimento di certificazione del credito verrà gestito a regime tramite una piattaforma elettronica (nel seguito sistema PCC, Piattaforma per la Certificazione dei Crediti) messa a disposizione dal Ministero dell'Economia e delle Finanze.
In attesa della piena realizzazione delle apposite funzionalità sulla piattaforma e, comunque, fino all'8 aprile 2013, le istanze di certificazione sono state presentate attraverso i canali tradizionali, utilizzando la modulistica allegata ai due "decreti certificazione" (c.d. procedura ordinaria).

Gli attori principali coinvolti nella certificazione dei crediti sono il **titolare del credito** (che chiameremo nel seguito creditore) e **l'amministrazione o ente debitore** (che chiameremo nel seguito P.A.), **i creditori subentranti** (le banche e gli intermediari finanziari, l'agente della riscossione), **altri soggetti**.

6.2 Il titolare del credito

Il creditore (o un suo delegato) dà inizio al processo di certificazione, presentando alla P.A., nei confronti della quale vanta un credito certificabile, un'istanza per la certificazione.
Se la P.A. non provvede al rilascio della certificazione entro 30 giorni dalla ricezione dell'istanza, il creditore può chiedere, all'Ufficio Centrale di Bilancio o alla Ragioneria Territoriale dello Stato, la nomina di un *commissario ad acta*, il quale provvederà al rilascio della suddetta certificazione in luogo della P.A.
Il creditore, ottenuta la certificazione, può recarsi presso una banca o un intermediario finanziario abilitato al fine di effettuare una cessione del credito ovvero per ottenere un'anticipazione a valere sullo stesso.
Può, altresì, recarsi presso una sede dell'Agente della riscossione e chiedere la compensazione del credito certificato con le somme dovute per tributi erariali, tributi regionali e locali, contributi assistenziali e previdenziali, premi per l'assicurazione obbligatoria contro gli infortuni e le malattie professionali, entrate spettanti alla P.A. che ha rilasciato la certificazione, notificati entro il 30 aprile 2012, nonché oneri accessori, aggi e spese e altre imposte la cui riscossione sia affidata all'Agente della riscossione.

6.3 L'amministrazione o ente debitore

La P.A. riceve le istanze di certificazione e, dopo aver effettuato gli opportuni riscontri, certifica il credito ovvero ne rileva l'inesigibilità o l'insussistenza, anche parziale.
Prima del rilascio della certificazione, per i crediti di importo superiore ai diecimila euro, la P.A. verifica presso l'Agente della riscossione l'eventuale presenza di accertate inadempienze

all'obbligo di versamento derivante dalla notifica di una o più cartelle di pagamento16. In caso si esito positivo di tale accertamento, la certificazione viene resa per l'intero credito, ma l'importo delle somme dovute all'Agente della riscossione viene annotato nella certificazione ed è vincolato al solo utilizzo ai fini della compensazione.
Nel caso in cui la P.A. vanti dei crediti nei confronti del richiedente, la certificazione sarà resa al netto di tali somme.
La P.A. risponde inoltre alle richieste di verifica presentate dall'Agente della riscossione o da una banca/intermediario finanziario, garantendo la sussistenza e la validità delle certificazioni.
Infine la P.A. effettua il pagamento del credito in favore del creditore originario (o di quello subentrato, nel caso di cessione o di compensazione) entro la data indicata sulla certificazione. Tale pagamento è registrato sul sistema PCC, riducendo il valore del credito certificato. Nel caso della procedura ordinaria, invece, il pagamento avviene previa restituzione della certificazione.

6.4 I creditori subentranti

A seguito dell'utilizzo della certificazione del credito ad opera del creditore originario, i seguenti soggetti possono diventare controparte della P.A.:
- le banche e gli intermediari finanziari abilitati ai sensi della legislazione vigente (nel seguito denominati istituti di credito) possono concedere anticipazioni o subentrare nel credito, in caso di cessione pro solvendo o pro soluto;
- l'Agente della riscossione interviene in caso di compensazione del credito certificato con somme dovute a seguito di iscrizione a ruolo.

6.5 Gli altri attori

Il processo di certificazione dei crediti coinvolge anche altri attori:
- gli Uffici Centrali di Bilancio - UCB (per le amministrazioni statali centrali e gli enti pubblici nazionali) e le Ragionerie Territoriali dello Stato - RTS (per le amministrazioni statali periferiche, le regioni, gli enti locali e gli enti del Servizio Sanitario Nazionale) provvedono entro 10 giorni dal ricevimento della relativa istanza alla nomina del *commissario ad acta*. Effettuano, inoltre, i riscontri previsti dalla normativa ai fini del rilascio della certificazione;
- i *commissari ad acta* sono nominati in caso di inerzia della P.A. Dopo aver effettuato le opportune verifiche, provvedono, entro 50 giorni dalla nomina, a certificare il credito o a dichiararne l'inesigibilità o l'insussistenza, anche parziale.

6.6 Accreditamento al sistema PCC (procedura telematica)

Gli attori descritti nei paragrafi precedenti che debbano utilizzare le apposite funzionalità del sistema PCC devono necessariamente accreditarsi alla piattaforma seguendo le indicazioni di seguito riportate.
Se il creditore è una società o un'impresa individuale, può operare in PCC direttamente il titolare o un suo rappresentante. Per potersi accreditare alla piattaforma, egli deve:

- inserire alcune informazioni personali;
- fornire la scansione di un valido documento d'identità;
- sottoscrivere una dichiarazione di assunzione di responsabilità;
- indicare quali società o imprese individuali rappresenti (alcuni dei dati sono reperiti automaticamente dal sistema mediante un collegamento con il Registro delle Imprese).

Le credenziali di accesso si compongono di due elementi distinti: il sistema PCC prevede, infatti, l'invio separato di tali elementi, rispettivamente, alla persona che ha effettuato l'accreditamento e alla casella di posta elettronica certificata (PEC), registrata sul Registro delle imprese, della società o impresa individuale rappresentata. Solo l'utilizzo congiunto di entrambi gli elementi consente di completare correttamente la registrazione sul sistema.
Se il creditore è una persona fisica (ad esempio un libero professionista) deve, preventivamente, effettuare un riconoscimento de visu, presso la P.A. e, con le credenziali di accesso ricevute, completare l'accreditamento al sistema PCC.
Ai sensi dell'art. 7 del D.L. n. 35/2013, a decorrere dall' 8 aprile 2013, data di entrata in vigore del d.l. n. 35/2013, la certificazione dei crediti è effettuata esclusivamente mediante la piattaforma elettronica. Pertanto le amministrazioni pubbliche, ai fini della certificazione delle somme dovute per somministrazioni, forniture ed appalti, devono provvedere a registrarsi entro il 28 aprile 2013. La mancata registrazione, oltre ad essere oggetto di valutazione della performance individuale dei dirigenti responsabili, comporta responsabilità dirigenziale e disciplinare nonché una sanzione pecuniaria pari a 100 euro per ogni giorno di ritardo.
Per le P.A. l'accreditamento al sistema PCC è effettuato a cura del Responsabile della P.A. secondo la procedura di seguito descritta:
- inserimento di alcune informazioni personali;
- scansione e trasmissione di un valido documento d'identità e dell'atto di nomina;
- sottoscrizione di una dichiarazione di assunzione di responsabilità;
- indicazione, eventuale, di dirigenti o funzionari titolari dei poteri per il rilascio delle certificazioni.

> Ai fini della procedura di certificazione dei crediti, per Responsabile della P.A. si intende un soggetto legittimato ad accreditarsi sul sistema PCC in nome e per conto della P.A. di appartenenza in virtù del ruolo in essa rivestito e titolare dei poteri necessari per rilasciare le certificazioni dei crediti ovvero per individuare le strutture e i dirigenti/funzionari che potranno svolgere tale funzione.
> Si forniscono, di seguito, alcune indicazioni utili per identificare correttamente il soggetto che dovrà accreditarsi quale Responsabile della P.A.
> Nel caso di pubbliche amministrazioni o enti con una struttura organizzativa particolarmente articolata, come le amministrazioni centrali dello Stato, le regioni e le province autonome, alcuni enti pubblici nazionali, per Responsabile della P.A. può intendersi il responsabile di ciascuna Area Organizzativa o il responsabile di ciascuna sede avente autonomia contabile, purché censita sull'Indice IPA.
> Nel caso delle amministrazioni periferiche dello Stato e della maggior parte degli enti pubblici nazionali, per Responsabile della P.A. deve intendersi il dirigente apicale (o figura equivalente) responsabile di ciascuna amministrazione o ente, che deve risultare censita sull'Indice IPA.
> Una volta accreditatosi, il Responsabile potrà individuare i Dirigenti/Responsabili delle strutture organizzative incaricati al rilascio delle certificazioni.

Le credenziali di accesso si compongono di due elementi distinti: il sistema PCC prevede, infatti, l'invio separato di tali elementi, rispettivamente, alla persona che ha effettuato l'accreditamento e alla casella di posta elettronica certificata, indicata su IPA, della P.A. rappresentata. Solo l'utilizzo congiunto di entrambi gli elementi consente di completare correttamente la registrazione sul sistema.
Nota bene: le P.A. debitrici possono accreditarsi al sistema PCC solo se già correttamente registrate nell'Indice Pubblica Amministrazione – IPA. In caso contrario, prima di dar luogo alla procedura sopra descritta occorre provvedere alla registrazione nel predetto indice. Maggiori informazioni sulla procedura da seguire sono reperibili sul sito Internet dell'IPA.

Il creditore, dopo aver effettuato l'accreditamento di cui sopra, inoltra l'istanza di certificazione del credito, utilizzando l'apposita funzionalità messa a disposizione dal sistema PCC.
Il sistema presenta all'utente un modulo, parzialmente precompilato con le informazioni relative al creditore già inserite in fase di registrazione, che deve essere completato specificando la P.A. nei confronti della quale si intende chiedere la certificazione, il dettaglio delle fatture a cui si riferisce il credito e la sottoscrizione delle dichiarazioni previste dalla normativa.
Il creditore ne riceve notifica della certificazione, o della rilevazione dell'insussistenza o inesigibilità del credito, all'indirizzo specificato di Posta Elettronica Certificata - PEC.
In ogni caso, il sistema permette di verificare, in ogni momento, lo stato di avanzamento del processo di certificazione e l'eventuale decorrenza dei termini per la richiesta di nomina di un *commissario ad acta*, per ciascuna istanza presentata.
Qualora la P.A. non provveda entro 30 giorni al rilascio della certificazione, o della rilevazione dell'insussistenza o inesigibilità, anche parziale, del credito, il creditore può presentare istanza di nomina di un commissario ad acta utilizzando l'apposita funzionalità messa a disposizione dalla piattaforma informatica.
Il sistema PCC propone un modulo precompilato con tutte le informazioni già inserite nell'istanza di certificazione alla quale ci si riferisce.
Il creditore riceve notifica sia dell'avvenuta nomina del commissario ad acta che del rilascio della certificazione, o della rilevazione dell'insussistenza o inesigibilità, anche parziale, del credito, all'indirizzo PEC specificato.
La P.A. o il commissario ad acta (nel caso sia stata presentata un'istanza di nomina a seguito di inerzia della P.A.) provvedono, dopo aver effettuato le opportune verifiche, a certificare che il credito sia certo, liquido ed esigibile o a rilevarne l'insussistenza o l'inesigibilità, anche parziale, utilizzando le apposite funzionalità del sistema PCC.
Il creditore ne riceve notifica **all'indirizzo PEC specificato.**
Il creditore, ottenuta la certificazione, può utilizzare il credito in diversi modi. In particolare:
- può effettuare la cessione, anche parziale, ovvero chiedere un'anticipazione a valere sullo stesso presso una banca o un intermediario finanziario abilitato;
- può chiedere all'Agente della riscossione la compensazione di tutto o parte del credito certificato con le somme dovute per i tributi, i contributi e gli altri debiti.

A tali fini il creditore deve recarsi presso la sede dell'istituto finanziario o dell'Agente della riscossione. Questi possono accedere al sistema PCC per verificare lo stato e la disponibilità del credito certificato.
È cura degli stessi istituti finanziari ovvero dell'Agente della riscossione registrare sul sistema PCC l'avvenuta operazione di cessione, anticipazione o compensazione effettuata a valere sul credito certificato.

Il sistema provvede automaticamente all'invio delle notifiche in formato elettronico a tutti gli attori interessati, i quali possono, in ogni momento, accedere alla piattaforma informatica per consultare lo stato e la disponibilità residua del credito. **In particolare, nel caso di cessione del credito, la comunicazione automatica inviata dal sistema alla P.A. ceduta assolve al requisito di cui all'articolo 117, commi 2 e 3, del decreto legislativo 12 aprile 2006, n. 163 e all'obbligo di notificazione.**

6.7 Procedura di ricognizione dei debiti contratti dalle pubbliche amministrazioni.

Particolarmente innovativa è la disposizione dell'art. 7 del d.l. n. 35/2013 che prevede l'obbligo per le pubbliche amministrazioni, a partire dal 1° giugno ed entro il termine del 15 settembre 2013, di comunicare attraverso l'utilizzo del sistema PCC, l'elenco completo dei debiti certi, liquidi ed esigibili maturati alla data del 31 dicembre 2012, con espressa indicazione dei dati identificativi del creditore. Il mancato adempimento dell'obbligo comporterà, per i dirigenti preposti, una responsabilità dirigenziale e disciplinare.
La predetta comunicazione dovrà avvenire utilizzando un apposito modulo messo a disposizione dalla piattaforma elettronica, nel quale sono separatamente specificati i crediti già oggetto di cessione o certificazione.
Il creditore può segnalare all'amministrazione pubblica debitrice, in tempo utile per il rispetto del termine previsto del 15 settembre 2013, l'importo e gli estremi identificativi del credito vantato nei confronti della stessa.
Per i crediti diversi da quelli oggetto di cessione o certificazione, la comunicazione effettuata dalla pubblica amministrazione equivale a tutti gli effetti giuridici ad una certificazione del credito.
In caso di omessa, incompleta o erronea comunicazione da parte della P.A. di uno o più debiti, il creditore può richiedere all'amministrazione di correggere o integrare la comunicazione del debito. Decorsi 15 giorni dalla data di ricevimento della richiesta senza che l'amministrazione abbia provveduto ovvero espresso un motivato diniego, il creditore può presentare istanza di nomina di un commissario ad acta, mediante la piattaforma elettronica, secondo le prescritte modalità.

7. Il Processo telematico

7.1 Notifica con modalità telematica

Di particolare interesse sono le novità introdotte dalla legge di stabilità alla legge 21 gennaio 1994, n. 53, disciplinando ex novo le modalità di notifica effettuate dagli Avvocati con modalità telematiche.
La notificazione telematica si effettua tramite pec soltanto agli indirizzi che risultano da pubblici elenchi. Per la notifica via pec da parte degli avvocati di atti non consistenti in documenti informatici, il legale ne estrae una copia informatica di cui attesta la conformità all'originale e l'atto così formato viene allegato al messaggio di posta elettronica certificata: anche in questo caso il momento di perfezionamento della notifica è quello che coincide con la generazione della ricevuta di avvenuta consegna del messaggio. Gli avvocati dovranno redigere la relazione

di notificazione su di un documento informatico separato, sottoscritto con firma digitale e allegato al messaggio inviato **via pec**: nel caso di notifica di atti non informatici, quindi, al messaggio di posta elettronica certificata dovranno essere allegati sia la copia informatica dello stesso atto sia la relazione di notificazione. Per l'atto notificato per via telematica il pagamento dell'importo corrispondente alla marca da bollo è effettuato con lo stesso mezzo informatico. In caso di malfunzionamento dei sistemi informatici del dominio "giustizia" il giudice può permettere il deposito cartaceo degli atti oppure ordinare il deposito di copia cartacea di singoli atti per ragioni specifiche.

7.2 Comunicazioni e notificazioni - uso mezzo telematico

È stabilito, altresì, l'obbligo per le cancellerie di usare esclusivamente il mezzo telematico per le comunicazioni e le notificazioni. Per gli uffici giudiziari, diversi da tribunali e corti d'appello, l'obbligo decorrerà dal quindicesimo giorno successivo a quello della pubblicazione nella Gazzetta Ufficiale dei decreti di natura non regolamentare con cui il ministro della Giustizia accerta la funzionalità dei servizi di comunicazione degli uffici. Nei procedimenti penali davanti a tribunali e corti d'appello, l'obbligo per le cancellerie di usare esclusivamente il mezzo telematico per le comunicazioni e le notificazioni a persona diversa dall'imputato decorrerà dal **15 dicembre 2014**.
Scatterà invece dal **30 giugno 2014** il deposito obbligatorio per via telematica degli atti processuali e dei documenti da parte dei difensori delle parti costituite nei procedimenti civili, contenziosi o di volontaria giurisdizione. La decorrenza dell'obbligo può essere anticipata nei tribunali in cui il ministro della Giustizia accerterà, con un decreto, la funzionalità dei servizi telematici.
Sul punto l'art. 1, comma 19, della legge di stabilità (l. n. 228/2012) modifica il decreto legge 18 ottobre 2012, n. 179, convertito con modificazioni con la legge 17 dicembre 2012, n. 221. In particolare l'art. 16 comma 12 prevede che *"Al fine di favorire le comunicazioni e notificazioni per via telematica alle pubbliche amministrazioni, le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni,* ***comunicano al Ministero della giustizia****, con le regole tecniche adottate ai sensi dell'articolo 4, comma 1, del decreto-legge 29 dicembre 2009, n. 193, convertito, con modificazioni, dalla legge 22 febbraio 2010, n. 24, entro centottanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto* ***l'indirizzo di posta elettronica certificata*** *conforme a quanto previsto dal decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e successive modificazioni,* ***a cui ricevere le comunicazioni e notificazioni. L'elenco formato dal Ministero della giustizia è consultabile esclusivamente dagli uffici giudiziari, dagli uffici notificazioni, esecuzioni e protesti, e dagli avvocati".***
Dopo l'art. 16 sono inseriti i seguenti :
«art. 16-bis. - (Obbligatorietà del deposito telematico degli atti processuali). - 1. Salvo quanto previsto dal comma 5, a decorrere dal 30 giugno 2014 nei procedimenti civili, contenziosi o di volontaria giurisdizione, innanzi al tribunale, il deposito degli atti processuali e dei documenti da parte dei difensori delle parti precedentemente costituite ha luogo esclusivamente con modalità telematiche, nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Allo stesso modo si procede per il deposito degli atti e dei documenti da parte dei soggetti nominati o delegati dall'autorità

giudiziaria. Le parti provvedono, con le modalità di cui al presente comma, a depositare gli atti e i documenti provenienti dai soggetti da esse nominati.
2. Nei processi esecutivi di cui al libro III del codice di procedura civile la disposizione di cui al comma 1 si applica successivamente al deposito dell'atto con cui inizia l'esecuzione.
3. Nelle procedure concorsuali la disposizione di cui al comma 1 si applica esclusivamente al deposito degli atti e dei documenti da parte del curatore, del commissario giudiziale, del liquidatore, del commissario liquidatore e del commissario straordinario.
4. A decorrere dal 30 giugno 2014, per il procedimento davanti al tribunale di cui al libro IV, titolo I, capo I, del codice di procedura civile, escluso il giudizio di opposizione, il deposito dei provvedimenti, degli atti di parte e dei documenti ha luogo esclusivamente con modalità telematiche, nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Il presidente del tribunale può autorizzare il deposito di cui al periodo precedente con modalità non telematiche quando i sistemi informatici del dominio giustizia non sono funzionanti e sussiste una indifferibile urgenza. Resta ferma l'applicazione della disposizione di cui al comma 1 al giudizio di opposizione al decreto d'ingiunzione.
5. Con uno o più decreti aventi natura non regolamentare, da adottarsi sentiti l'Avvocatura generale dello Stato, il Consiglio nazionale forense ed i consigli dell'ordine degli avvocati interessati, il Ministro della giustizia, previa verifica, accerta la funzionalità dei servizi di comunicazione, individuando i tribunali nei quali viene anticipato, anche limitatamente a specifiche categorie di procedimenti, il termine previsto dai commi da 1 a 4.
6. Negli uffici giudiziari diversi dai tribunali le disposizioni di cui ai commi 1 e 4 si applicano a decorrere dal quindicesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale della Repubblica italiana dei decreti, aventi natura non regolamentare, con i quali il Ministro della giustizia, previa verifica, accerta la funzionalità dei servizi di comunicazione. I decreti previsti dal presente comma sono adottati sentiti l'Avvocatura generale dello Stato, il Consiglio nazionale forense ed i consigli dell'ordine degli avvocati interessati.
7. Il deposito di cui ai commi da 1 a 4 si ha per avvenuto al momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del Ministero della giustizia.
8. Fermo quanto disposto al comma 4, secondo periodo, il giudice può autorizzare il deposito degli atti processuali e dei documenti di cui ai commi che precedono con modalità non telematiche quando i sistemi informatici del dominio giustizia non sono funzionanti.
9. Il giudice può ordinare il deposito di copia cartacea di singoli atti e documenti per ragioni specifiche.

L'art. 16-ter, rubricato *"Pubblici elenchi per notificazioni e comunicazioni",* ha specificato che ai fini della notificazione e comunicazione degli atti in materia civile, penale, amministrativa e stragiudiziale si intendono per pubblici elenchi quelli previsti da:

- L'anagrafe nazionale della popolazione residente - ANPR, (art. 3-bis del C.A.D.).
  L'elenco formato dal Ministero della Giustizia al quale le amministrazioni pubbliche hanno comunicato l'indirizzo di PEC a cui ricevere le comunicazioni e notificazioni (art. 16, comma 12, del decreto-legge 179/2012).
- Il registro delle imprese, al quale le imprese costituite in forma societaria sono tenute a indicare il proprio indirizzo di PEC, l'elenco riservato (consultabile in via telematica esclusivamente dalle pubbliche amministrazioni) tenuto dagli ordini e dai collegi al quale i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato devono comunicare il

proprio indirizzo di PEC e l'elenco tenuto dall'Agenzia per l'Italia digitale alla quale le amministrazioni pubbliche hanno comunicato il proprio indirizzo di PEC (art. 16 del decreto-legge n. 185/2008, convertito con modificazioni dalla legge n. 2/2009).
- L'Indice nazionale degli indirizzi di posta elettronica certificata (INI-PEC) delle imprese e dei professionisti, presso il Ministero per lo sviluppo economico, realizzato a partire dagli elenchi di indirizzi PEC costituiti presso il registro delle imprese e presso gli ordini o collegi professionali, cui possono accedere le pubbliche amministrazioni, i professionisti, le imprese, i gestori o esercenti di pubblici servizi e tutti i cittadini tramite sito web e senza necessità di autenticazione. (art 6-bis del decreto legislativo n. 82/2005).
- Il registro generale degli indirizzi elettronici gestito dal Ministero della Giustizia.

8. Le procedure concorsuali

L'articolo 17 del decreto- legge n. 179/2012 convertito dalla legge n. 221/2012 e l'articolo 1, comma 19, della legge n. 228/2012 (legge di stabilità) hanno introdotto rilevanti novità nella disciplina delle procedure concorsuali.
In particolare la prima disposizione ha introdotto la **posta elettronica certificata** per la notifica degli atti previsti nelle procedure concorsuali, mentre la seconda ha apportato modifiche in tema di comunicazione al registro delle imprese del proprio indirizzo di posta elettronica certificata da parte dei curatori, dei commissari giudiziali e dei commissari liquidatori.

Nell'ambito delle misure dirette alla realizzazione del "*processo telematico*", le disposizioni in argomento hanno inserito la posta elettronica certificata (PEC) nelle procedure concorsuali, con l'intento di velocizzare le comunicazioni e contenere i costi della giustizia.
L'articolo 17 del decreto-legge n. 179/2012 convertito, con modificazioni, dalla legge n. 221/2012, ha compreso nuove disposizioni nella legge fallimentare e modificato alcune già esistenti.
I commi 3, 4 e 5, hanno disciplinato la decorrenza dell'applicazione delle nuove disposizioni.
Alcune di queste si applicano, dal **19 dicembre 2012** (data di entrata in vigore della legge di conversione n. 221/2012), anche alle procedure di fallimento, di concordato preventivo, di liquidazione coatta amministrativa e di amministrazione straordinaria pendenti, per le quali alla stessa data non è stata effettuata la comunicazione prevista dagli articoli 92, 171, 207 della legge fallimentare e dall'art. 22 del decreto legislativo n. 270/1999.
Per le procedure in cui al 19 dicembre 2012 sono state, invece, effettuate le citate comunicazioni, le nuove disposizioni si applicano dal **31 ottobre 2013**.
Di particolare rilievo è la disposizione che ha previsto l'obbligo del curatore, del commissario giudiziale, del commissario liquidatore e del commissario straordinario di comunicare, entro il **30 giugno 2013**, ai creditori e ai terzi titolari di diritti sui beni il loro indirizzo di posta elettronica certificata e li invitano a comunicare, entro tre mesi, l'indirizzo di posta elettronica certificata al quale ricevere tutte le comunicazioni relative alla procedura, avvertendoli di rendere nota ogni successiva variazione e che in caso di omessa indicazione le comunicazioni sono eseguite esclusivamente mediante deposito in cancelleria.
A tal fine la legge di stabilità 2013 ha previsto l'obbligo per il curatore, il commissario giudiziale, il commissario liquidatore e il commissario giudiziale di comunicare al registro delle imprese, entro dieci giorni dalla nomina, il proprio indirizzo di PEC.

Per quanto riguarda le modifiche apportate alla legge fallimentare, si sintetizzano di seguito le principali novità:

a. nel procedimento per la dichiarazione di fallimento (art. 15 L.F.), il ricorso e il decreto di convocazione devono essere notificati, a cura della cancelleria, all'indirizzo PEC del debitore risultante dal registro delle imprese ovvero dall'INI-PEC. L'esito della comunicazione è trasmesso, con modalità automatica, all'indirizzo di posta elettronica certificata del ricorrente. Se per qualsiasi regione la notificazione non risulta possibile o non ha esito positivo, la notifica a cura del ricorrente del ricorso e del decreto si esegue esclusivamente di persona in base all'art. 107, 1° comma, del D.P.R. 1229/1959 presso la sede risultante dal registro delle imprese. Se nemmeno tale modalità può essere attuata, la notifica si esegue con il deposito dell'atto nella casa comunale della sede che risulta iscritta nel registro delle imprese. La disposizione si applica ai procedimenti introdotti dopo il 31 dicembre 2013.
b. Le comunicazioni del curatore ai creditori sono effettuate all'indirizzo PEC da loro indicato (art. 31-bis). In caso di omessa indicazione o di mancata consegna del messaggio PEC per cause imputabili al destinatario, tutte le comunicazioni sono eseguite esclusivamente mediante deposito in cancelleria. Anche il rapporto riepilogativo delle attività svolte dal curatore è trasmesso a mezzo PEC ai creditori (art. 33).
c. L'avviso ai creditori (art. 92) è trasmesso anch'esso dal curatore a mezzo PEC se il relativo indirizzo del destinatario risulta dal registro delle imprese ovvero dall'INI-PEC e, in ogni altro caso, a mezzo lettera raccomandata o telefax presso la sede dell'impresa o la residenza del creditore e nell'avviso deve essere indicato l'indirizzo PEC del curatore stesso.
d. Il ricorso con cui si propone la domanda di ammissione al passivo di un credito (art. 93) è trasmesso all'indirizzo PEC del curatore indicato nell'avviso di cui all'art. 92. Nel ricorso il creditore deve indicare l'indirizzo PEC al quale ricevere tutte le comunicazioni relative alla procedura, ***"le cui variazioni è onere comunicare al curatore"***.
e. Il curatore trasmette il progetto di stato passivo ai creditori all'indirizzo PEC indicato nella domanda di insinuazione al passivo (art. 95), con le stesse modalità è trasmesso ai creditori il progetto di ripartizione delle somme disponibili (art. 110) e il rendiconto del curatore (art. 116).
f. Analoghe disposizioni sono state introdotte per il concordato, in particolare la proposta di concordato, quando è presentata da un terzo, deve indicare l'indirizzo PEC al quale ricevere le comunicazioni (art. 125) ed è comunicata dal curatore ai creditori a mezzo PEC. In caso di approvazione della proposta, il giudice delegato dispone che il curatore ne dia immediata comunicazione a mezzo PEC al proponente (art. 129).
g. In tema di esdebitazione (art. 143) è previsto che il ricorso e il decreto siano comunicati dal curatore ai creditori a mezzo PEC.
h. Con riferimento al concordato preventivo e agli accordi di ristrutturazione, per quanto riguarda la convocazione dei creditori e il relativo avviso (art. 171) è previsto che il commissario giudiziale effettui la comunicazione ai creditori a mezzo posta elettronica certificata, se il relativo indirizzo del destinatario risulta dal registro delle imprese ovvero dall'INI-PEC e, in ogni altro caso, a mezzo lettera raccomandata o telefax presso la sede dell'impresa o la residenza del creditore. Anche in questo caso, è previsto che il commissario giudiziale comunichi il suo indirizzo di posta elettronica certificata, invitando i creditori ad indicare un indirizzo PEC. Anche la relazione del commissario giudiziale (art. 172) deve essere comunicata via PEC ai creditori, così come la comunicazione di apertura del procedimento per la revoca dell'ammissione al concordato (art. 173) nonché il rapporto del liquidatore previsto nel concordato consistente nella cessione dei beni (art. 182).

i. Analoghe disposizioni sono state previste con riguardo alla liquidazione coatta amministrativa (articoli 205, 207, 208, 209 e 213).

La materia in esame è stata successivamente modificata dall'art. 1, comma 19, della legge di stabilità 2013 che ha inserito l'art. 16-bis al decreto-legge n. 179/2012.
La disposizione ha previsto (cfr. supra par. 7.2) che a decorrere dal **30 giugno 2014** nei procedimenti civili, contenziosi o di volontaria giurisdizione innanzi al tribunale, il deposito telematico degli atti processuali e dei documenti da parte dei difensori ha luogo esclusivamente con modalità telematiche.
Il comma 3 dispone che nelle procedure concorsuali tale obbligo si applica esclusivamente al deposito degli atti e dei documenti da parte del curatore, del commissario giudiziale, del liquidatore, del commissario liquidatore e del commissario straordinario e che il deposito degli atti si ha per avvenuto al momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del Ministero della giustizia (comma 7).

9. I pignoramenti presso terzi

In tema di espropriazione presso terzi è prescritta dall'art. 543 c.p.c. l'indicazione dell'indirizzo di **posta elettronica certificata** del creditore procedente.
In proposito si osserva che ai sensi degli artt. 4 e 5 del D.L. 18 ottobre 2012 n. 179, convertito con modificazioni dalla legge 17 dicembre 2012 n. 221, la Pec è obbligatoria anche per le imprese individuali.
Infatti a partire dal 20 ottobre 2012 le imprese che si iscrivono per la prima volta al Registro delle Imprese devono richiedere immediatamente la casella Pec per il contestuale deposito.
Per le imprese individuali già esistenti, l'indirizzo PEC deve essere, invece, depositato al Registro delle Imprese entro il 30 giugno 2013.
Inoltre, per quanto riguarda i singoli cittadini si evidenzia che ai sensi dell'art. 3 bis del CAD (introdotto dall'art. 4, comma 1, D.L. 18 ottobre 2012 n. 179), dal 1° gennaio 2013, è istituito il "**domicilio digitale del cittadino**" (v. supra par. 3.1).
È novellato, pertanto, anche l'articolo 547 c.p.c.: oltre che la classica raccomandata, ora il terzo può utilizzare anche un messaggio di posta elettronica certificata inviato al creditore procedente per specificare di quali somme o di quali cose sia debitore o si trova in possesso (e quando ne debba eseguire il pagamento o la consegna).
L'articolo 548 c.p.c. detta la nuova disciplina sulla mancata dichiarazione del terzo: nel caso di crediti alimentari, se il pignoramento riguarda (per la parte "esecutabile") le somme dovute dai privati a titolo di stipendio, di salario o di altre indennità relative al rapporto di lavoro o di impiego comprese quelle dovute a causa di licenziamento, la mancata comparizione del terzo all'udienza equivale a mancata contestazione del credito pignorato ai fini del procedimento in corso oltre che dell'esecuzione fondata sul provvedimento di assegnazione; in tal caso il giudice dell'esecuzione provvede con ordinanza all'assegnazione dei crediti in pagamento ai creditori concorrenti (ex articoli 552 e 553 c.p.c.).
Fuori dei casi indicati, se all'udienza il creditore dichiara di non avere ricevuto la dichiarazione del terzo, il giudice fissa con ordinanza una nuova udienza: laddove il terzo non compare nuovamente, il credito pignorato o il possesso del bene di appartenenza del debitore si considera non contestato.

L'ordinanza di assegnazione dei crediti adottata dal giudice dell'esecuzione sulla base delle previsioni dell'articolo 648 c.p.c. è impugnabile dal terzo soltanto se egli prova di non averne avuto tempestiva conoscenza per irregolarità della notificazione, per caso fortuito o per forza maggiore: il termine previsto è pari a venti giorni e decorre dalla notificazione dell'ordinanza.
Cambia anche l'articolo 549 c.p.c.: le contestazioni sulla dichiarazione del terzo sono risolte dal giudice dell'esecuzione, previo accertamento, con ordinanza impugnabile come per l'articolo 548 c.p.c..
L'ordinanza ha effetto ai fini del procedimento in corso e dell'esecuzione fondata sul provvedimento di assegnazione.
La nuova disciplina è applicabile ai procedimenti di esecuzione presso terzi iniziati dopo il **1° gennaio 2013**.

9.1 Ricevuta elettronica

Nei processi di esecuzione l'obbligatorietà decorre dal deposito dell'atto con cui inizia l'esecuzione; nelle procedure concorsuali, il deposito telematico riguarda gli atti e documenti da parte del curatore, del commissario giudiziale e del commissario straordinario. Il deposito si considera avvenuto al momento in cui il gestore della posta elettronica certificata del ministero della Giustizia genera la ricevuta di avvenuta consegna. Nei procedimenti d'ingiunzione davanti al tribunale, a partire dal 30 giugno 2014, il deposito dei provvedimenti, degli atti di parte e dei documenti avverrà esclusivamente con modalità telematiche (escluso il giudizio di opposizione al decreto ingiuntivo dove l'obbligo di deposito "telematico" vale solo per gli atti provenienti dai difensori). Il deposito con modalità diverse può essere autorizzato dal tribunale solo se non risultano funzionanti i sistemi informatici del dominio giustizia o in caso di estrema urgenza. Per gli uffici giudiziari diversi dai tribunali il deposito telematico diventa obbligatorio quindici giorni dopo la pubblicazione in Gazzetta Ufficiale dei provvedimenti del Ministero di Giustizia che accertano la funzionalità dei servizi di comunicazione degli uffici.

10. Conclusioni

La normativa sul documento informatico e sulla firma elettronica sin qui esaminata trova la sua giustificazione sia nell'opportunità di snellire al massimo i rapporti tra privati e la pubblica amministrazione, sia, più in generale, nella constatazione che, ormai, alla corrispondenza epistolare tradizionale e all'uso della posta si è sostituito sempre più l'uso della posta elettronica (certificata o meno).
L'utilizzo e la diffusione della Firma Digitale e della Posta Elettronica Certificata sono stati negli ultimi anni degli obiettivi prioritari dell'azione di governo Italiano nell'ambito dei processi di semplificazione amministrativa. La firma digitale, infatti, è indispensabile nell'automazione dei processi amministrativi, nella gestione informatizzata dei flussi documentali e in tutti quei procedimenti dove si vuole l'eliminazione del documento cartaceo (smaterializzazione del procedimento amministrativo), mentre la PEC rappresenta ormai lo strumento più rapido e sicuro di trasmissione documentale.
Sono ormai numerose le applicazioni che utilizzano la firma digitale e la PEC nell'ambito della pubblica amministrazione. Applicazioni che coinvolgono sempre più:

- le imprese, con l'obbligo di trasmissione telematica di atti e documenti;
- la pubblica amministrazione, con la piena smaterializzazione dei flussi provvedimentali ormai firmati e trasmessi elettronicamente;
- i cittadini, con la possibilità, già descritta precedentemente, di inviare istanze e dichiarazioni alla pubblica amministrazione in modalità telematica.

I professionisti saranno sempre più coinvolti nell'utilizzo della firma digitale per gli atti notarili, per gli atti giudiziari nell'ambito del processo telematico e per le dichiarazioni fiscali.
Occorre, infatti, sostituire all'autografia, come mezzo di prova, altri sistemi che assicurano la provenienza, l'integrità e la riservatezza dei messaggi scritti. Solo così, invero, il pubblico li userà anche nella versione informatica, con sicurezza e fiducia. Si tratta, quindi, di incidere profondamente nella cultura, nelle consuetudini, nelle convinzioni, più radicate nella collettività.
Sotto questo aspetto, la disciplina del documento informatico e della firma elettronica va oltre il valore tecnico-giuridico di una semplice innovazione tecnologica di settore: è una rivoluzione, più che una evoluzione.
La diffusione della Carta d'Identità Elettronica, della Carta Nazionale dei Servizi e da ultimo della chiavetta USB (c.d. Token) non potrà che favorire ulteriormente lo sviluppo e il conseguente utilizzo della firma digitale da parte dei cittadini.
A livello internazionale bisogna dare maggiore impulso alle attività finalizzate a garantire l'interoperabilità delle procedure tecnologiche, almeno tra i paesi dell'Unione, e in questo senso è stato avviato, negli ultimi anni, da parte degli organismi europei, un concreto processo di regolamentazione.
Anche sotto quest'ultimo aspetto la legislazione italiana, così come emerge dalla lettura delle norme del "Codice", risulta essere all'avanguardia. Basti considerare che l'art. 71, comma 1ter, stabilisce che le regole tecniche del CAD devono essere dettate in conformità *"alle discipline risultanti dal processo di stantardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea*".

APPENDICE

Documenti

- Direttiva europea 1999/93/CE sulle firme elettroniche - *"Directive 1999/93/EC of the European Parliament and of the Council on a common framework for electronic signatures".*
- Legge 21 gennaio 1994, n. 53 - "*Facoltà di notificazioni di atti civili, amministrativi e stragiudiziali per gli avvocati e procuratori legali*".
- Decreto del Presidente della Repubblica 28 dicembre 2000 n. 45 "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*".
- Decreto legislativo 23 gennaio 2002, n. 10 - "*Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche*" - **abrogato a decorrere dal 1° gennaio 2006, per effetto dell'articolo 75 del D.LGS. 7 marzo 2005, n. 82**;
- Decreto del Presidente della Repubblica 7 aprile 2003, n. 137 *"Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del decreto legislativo 23 gennaio 2002, n. 10"*.
- Legge 16 gennaio 2003 n. 3, *"Disposizioni ordinamentali in materia di pubblica amministrazione"*- art. 27.
- Decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003 n. 14142 *"Approvazione dello schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art. 10, comma 1, del decreto legislativo 23 febbraio 2002, n. 10";*
- Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 n. 14146 "*Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici*" **abrogato dall'articolo 53, comma 2, del D.P.C.M. 30 marzo 2009 n. 38840***.*
- Deliberazione CNIPA (oggi Agenzia per l'Italia digitale, ex DigitPA) n. 4 del 17 febbraio 2005 *"Regole per il riconoscimento e la verifica del documento informatico"*.
- Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 *"Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3."*;
- Decreto Legislativo 7 marzo 2005, n. 82 *"Codice dell'Amministrazione Digitale"* C.A.D..
- Decreto Ministeriale 2 novembre 2005 n. 19818 *"Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata*", con Allegate *«Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata»;*
- Circolare CNIPA n. 49 del 24 novembre 2005 *"Modalità per la presentazione delle domande di iscrizione all'elenco pubblico dei gestori di posta elettronica certificata*";
- Circolare CNIPA 7 dicembre 2006, n. 51 *"Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di posta elettronica certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3»*".
- Decreto Legge 29 novembre 2008, n. 185, convertito nella Legge 28 gennaio 2009, n. 2 - "*Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale".* (c.d. Decreto Anticrisi).

- Decreto del Presidente del Consiglio dei ministri del 30 marzo 2009 n. 38840 *"Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici",* **ora sostituito dal DPCM 22 febbraio 2013, n. 68380**.
- Guida alla Firma Digitale - CNIPA aprile 2009.
- Decreto del Presidente del Consiglio dei ministri del 6 maggio 2009, n. 38524 *"Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini".*
- Deliberazione CNIPA 21 maggio 2009, n. 45, come modificata ed integrata dalla Determinazione Commissariale DIGIT.PA n. 69 del 28 luglio 2010 *"Regole per il riconoscimento e la verifica del documento informatico"*
- Decreto del Presidente del Consiglio dei ministri 10 febbraio 2010 n. 45232 "*Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza"*.
- Comunicato DIGITPA 27 maggio 2010 n. 45895 - Attuazione delle disposizioni di cui all'articolo 39 del decreto del Presidente del Consiglio dei Ministri 30 marzo 2009: *"Codici identificativi delle chiavi pubbliche relative alle coppie di chiavi utilizzate per la sottoscrizione dell'Elenco pubblico dei certificatori accreditati per la firma digitale*" e del decreto 24 luglio 2009: *"Modifica dell'allegato al decreto del Ministro dell'interno, del Ministro dell'economia e delle finanze e del Ministro per l'innovazione e le tecnologie del 9 dicembre 2004, recante: Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi"*.
- Decreto del Ministro della Giustizia 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, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24"*.
- Decreto del Presidente del Consiglio dei ministri del 22 luglio 2011 n. 56784 *"Comunicazioni con strumenti informatici tra imprese e amministrazioni pubbliche, ai sensi dell'articolo 5-bis del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni".*
- Decreto legge 09 febbraio 2012, n. 5 convertito, con modificazioni nella legge n. 35 del 04 aprile 2012 *"Disposizioni urgenti in materia di semplificazioni e sviluppo"* - art. 20.
- Decreto del Presidente del Consiglio dei ministri 19 luglio 2012 n. 63811 "*Definizione dei termini di validità delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003, e dei termini per la sostituzione dei dispositivi automatici di firma*".
- Decreto del Presidente del Consiglio dei ministri del 27 settembre 2012 n. 65329 *"Regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata, ai sensi dell'articolo 65, comma 1, lettera c-bis), del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005 n. 82 e successive modificazioni".*
- Decreto del Ministro della Giustizia 15 ottobre 2012 n. 209 - Regolamento recante: "*Regole tecniche per l'adozione nel processo civile e penale delle tecnologie dell'informazione e comunicazione - modifiche al decreto ministeriale 21 febbraio 2011, n. 44"*.
- Decreto legge 18 ottobre 2012, n. 179 *"Ulteriori misure urgenti per la crescita del Paese"* (c.d. Sviluppo bis), convertito nella legge 17.12.2012, n. 221.

- Legge 6 novembre 2012, n. 190 *"Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"*, art. 1, commi 29/30;
- Legge 24 dicembre 2012, n. 228 (legge di stabilità 2013).
- Decreto Legge 08 aprile 2013, n. 35 *"Disposizioni urgenti per il pagamento dei debiti scaduti della pubblica amministrazione, per il riequilibrio finanziario degli enti territoriali, nonché in materia di versamento di tributi degli enti locali"*.
- Decreto del Ministero dello Sviluppo Economico (MISE) 19 marzo 2013, pubblicato nella G.U. n. 83 del 09 aprile 2013, *"Indice degli indirizzi di posta elettronica certificata delle imprese e dei professionisti*".
- Decreto del Ministro della Giustizia 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 penale delle tecnologie dell'informazione e della comunicazione*".
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013, n. 68380, pubblicato nella G.U. n. 117 del 21 maggio 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"*.

- Circolari Inail:
- n. 1 del 10 gennaio 2012.
- n. 43 del 14 settembre 2012.
- n. 59 del 31 ottobre 2012.
- n. 61 del 09 novembre 2012.
- nn. 68/69 del 21 dicembre 2012.
- n. 19 dell'11 aprile 2013.

- artt. 543 e ss. C.p.c.

- D.M. MEF 22 maggio 2012 n. 61398 e successive modificazioni.
- Circolare MEF n. 35 del 27 novembre 2012.