

Marcello De Geronimo - Giovanni Mastriforti

# Guida introduttiva ai servizi telematici per l'Avvocatura

---

© Marcello De Geronimo, Giovanni Mastriforti, 2010 – Alcuni diritti riservati

Quest'opera è utilizzabile secondo i termini della licenza Creative Commons Attribuzione-Non commerciale-Condividi allo stesso modo 2.5 Italia e può essere liberamente riprodotta dagli iscritti all'Ordine degli Avvocati di Catania quale supporto formativo per la propria attività professionale.

*Indice generale*

<a href="#">1 Cronologia delle modifiche apportate.....</a>	<a href="#">3</a>
<a href="#">2 Acronimi.....</a>	<a href="#">3</a>
<a href="#">3 Documentazione e normativa di riferimento.....</a>	<a href="#">3</a>
<a href="#">4 Premessa.....</a>	<a href="#">4</a>
<a href="#">5 Concetti di base.....</a>	<a href="#">5</a>
<a href="#">5.1 Definizioni.....</a>	<a href="#">5</a>
<a href="#">5.2 Alcune errate convinzioni da debellare.....</a>	<a href="#">6</a>
<a href="#">5.3 La dematerializzazione.....</a>	<a href="#">6</a>
<a href="#">6 Servizi di consultazione.....</a>	<a href="#">9</a>
<a href="#">7 La Posta Elettronica Certificata (PEC).....</a>	<a href="#">10</a>
<a href="#">8 Il Punto d'Accesso al Processo Telematico (PdA).....</a>	<a href="#">15</a>

*Indice tabelle*

Tabella 1 – Cronologia modifiche.....	3
Tabella 2 - Acronimi.....	3
Tabella 3 - Tabella di corrispondenza per l'attuazione della dematerializzazione.....	7

## 1 Cronologia delle modifiche apportate

Versione	Modifiche apportate
1.0 - 5 gennaio 2010	Primo rilascio
1.1 - 6 gennaio 2010	Rivista la definizione di certificato digitale. Correzioni minori.

Tabella 1 – Cronologia modifiche

## 2 Acronimi

Acronimo	Nome esteso
CA	Certification Authority (autorità di certificazione)
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione. Dall'1 dicembre 2009, il CNIPA ha assunto la denominazione "DigitPA".
CPEPCT	Casella di Posta Elettronica Certificata del Processo Telematico, recentemente ribattezzata "Casella PEC-PCT".
CNS	Carta Nazionale dei Servizi.
PCT	Processo Civile Telematico.
PdA	Punto d'Accesso al Processo Telematico.
PEC	Posta Elettronica Certificata.
PEC-PCT	Posta Elettronica Certificata per il Processo Civile Telematico.
S/MIME	Secure Multipurpose Internet Mail Extensions.

Tabella 2 - Acronimi

## 3 Documentazione e normativa di riferimento

### **Documento informatico:**

[http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Firma\\_digitale/Cos%27%C3%A8\\_la\\_firma\\_digitale/Il\\_documento\\_informatico/](http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Firma_digitale/Cos%27%C3%A8_la_firma_digitale/Il_documento_informatico/)  
[http://www.cnipa.gov.it/site/it-IT/Normativa/Raccolta\\_normativa ICT/Documento\\_informatico/](http://www.cnipa.gov.it/site/it-IT/Normativa/Raccolta_normativa ICT/Documento_informatico/)

### **Firma digitale qualificata:**

[http://www.cnipa.gov.it/site/it-IT/Attività/Firma\\_digitale/](http://www.cnipa.gov.it/site/it-IT/Attività/Firma_digitale/)

### **Conservazione sostitutiva:**

[http://www.cnipa.gov.it/site/files/DELIBERAZIONE%2019%20febbraio%202004\\_v1.pdf](http://www.cnipa.gov.it/site/files/DELIBERAZIONE%2019%20febbraio%202004_v1.pdf)  
<http://www.conservazionesostitutiva.it/index/normativa>

### **Carta Nazionale dei Servizi:**

[http://www.cnipa.gov.it/site/it-IT/Attività/Firma\\_digitale/Certificatori\\_accreditati/Carta\\_Nazionale\\_dei\\_Servizi/Normativa/](http://www.cnipa.gov.it/site/it-IT/Attività/Firma_digitale/Certificatori_accreditati/Carta_Nazionale_dei_Servizi/Normativa/)

### **Posta Elettronica Certificata:**

[http://www.cnipa.gov.it/site/it-IT/Attività/Posta\\_Elettronica\\_Certificata\\_\(PEC\)/](http://www.cnipa.gov.it/site/it-IT/Attività/Posta_Elettronica_Certificata_(PEC)/)

### **Processo Civile Telematico:**

<http://www.processotelematico.giustizia.it/pdapublic/index.jsp?sid=1&id=4&pid=4>

## 4 Premessa

Nell'espletare l'attività di supporto agli Avvocati, abbiamo rilevato una comprensibile difficoltà da parte del singolo Iscritto nell'approccio ai *servizi telematici* e alla *dematerializzazione*, la cui attuazione sembra divenuta imminente e inarrestabile.

Per aiutare l'Iscriito armato di buona volontà a dipanare la matassa abbiamo redatto il presente documento, che propone innanzitutto i concetti di base che ci sembrano imprescindibili per usufruire consapevolmente dei servizi telematici per l'Avvocatura, per poi fornire un sommario quadro d'insieme, ponendo maggiore attenzione sui temi più attuali: la Posta Elettronica Certificata e il Processo Civile Telematico.

## 5 Concetti di base

### 5.1 Definizioni

- **Documento informatico:** rappresentazione digitale di fatti o dati giuridicamente rilevanti.
- **Certificato digitale:** documento informatico rilasciato e firmato digitalmente da un'autorità attendibile (*autorità di certificazione, CA*) che attesta l'identità di un soggetto (una persona, una società, un computer, etc).

Un certificato digitale contiene, oltre ai dati identificativi del titolare, una **chiave pubblica**, adoperabile per vari scopi. Ad esempio una chiave pubblica consente al destinatario di un documento informatico firmato digitalmente di **verificare l'autenticità della firma digitale**. Oppure può essere usata per **cifrare** un documento informatico, di modo che solo il titolare del certificato possa decifrarlo.

Ad una *chiave pubblica* corrispondente univocamente una **chiave privata**. Quest'ultima, custodita in un computer o in un dispositivo, tipicamente una tessera elettronica (*smart card*) di dimensioni ridotte, consente al titolare del certificato sia di **firmare digitalmente** un documento informatico, sia di **decifrare** i documenti informatici cifrati con la corrispondente *chiave pubblica*.

Gli usi possibili di un certificato digitale, con la chiave privata ad esso associata, sono pertanto vari (documento di riconoscimento, sottoscrizione di documenti informatici, produzione di documenti leggibili solo dal destinatario) e tecnicamente un'autorità di *certificazione* può impostare un certificato per tutti gli usi, ma la legge prevede che i certificati di firma qualificata siano dedicati esclusivamente a questa funzione.

- **Impronta (di un documento informatico):** rappresentazione sintetica e univoca di un documento informatico.

L'impronta si ottiene applicando al documento un procedimento matematico che garantisce l'univoca corrispondenza fra i due oggetti. Documenti differenti hanno impronte differenti. Impronte identiche sono riconducibili esclusivamente allo stesso documento.

- **Firma digitale:** sottoscrizione dell'impronta di un documento informatico.

Consiste nella cifratura dell'impronta per mezzo di una "chiave" posseduta esclusivamente dal firmatario (*chiave privata*).

Un *file firmato* contiene tre oggetti: il documento originale, l'impronta del documento firmata digitalmente (impronta cifrata) e il *certificato di firma digitale* del sottoscrittore.

Il certificato di firma digitale attesta l'autenticità della *firma* del sottoscrittore, poiché contiene la *chiave pubblica* che consente di risalire all'impronta (più esattamente, consente di decifrare l'impronta firmata) e di verificare la corrispondenza dell'impronta stessa con il documento informatico.

I software di firma digitale, distribuiti gratuitamente dalle *autorità di certificazione*, consentono di eseguire agevolmente queste verifiche.

- **Autenticazione:** l'operazione di riconoscimento di un soggetto da parte di un sistema, per consentire l'accesso del soggetto stesso a dati e servizi di sua pertinenza.

La verifica dell'identità del soggetto tipicamente avviene tramite l'inserimento di un nome (più comunemente uno pseudonimo o *nome utente*) e di una parola d'ordine (*o password*), che il soggetto deve custodire responsabilmente per evitare il furto d'identità. Sistemi che richiedono maggiori garanzie usano tecniche di identificazione più sofisticate. Ad esempio il Processo Civile Telematico e l'accesso ai Registri della Corte di Cassazione richiedono l'uso di un sistema di *autenticazione forte*, basato sull'uso di un *certificato di autenticazione* e della relativa *chiave privata*, con quest'ultima custodita in un dispositivo da cui non può essere estratta, ma solamente adoperata previo inserimento di un codice segreto numerico (PIN).

- **Cifratura:** codifica di un documento informatico, allo scopo di renderlo leggibile solo alle persone autorizzate a leggerlo.

L'uso della cifratura consente di inviare documenti informatici con il massimo grado di riservatezza: cifrando un documento usando la chiave pubblica del destinatario, solo quest'ultimo può leggerne il contenuto, operando la decodifica tramite la propria chiave privata.

L'operazione di cifratura ha l'effetto di raddoppiare (all'incirca) la dimensione del documento originale.

- **Posta Elettronica Certificata (PEC): sistema di posta elettronica che fornisce prova opponibile dell'invio e della consegna di un documento informatico.**

Il sistema PEC "certifica" anche la provenienza e l'integrità del messaggio, oltre che gli orari di invio e di ricezione del messaggio stesso.

## 5.2 Alcune errate convinzioni da debellare

I concetti appena esposti consentono di ribaltare alcune convinzioni che, per quanto abbiamo rilevato, si radicano spontaneamente nella mente del giurista che non ha ancora avuto occasione di approfondire questi temi.

- Nell'ambito dei Servizi Telematici, il termine "autenticazione" non va associato al concetto di "firma autenticata" (ovvero l'attestazione, da parte di un pubblico ufficiale, che la firma autografa è stata apposta in sua presenza da una persona di cui ha accertamento l'identità).

- Non si accede ad un sistema con la firma digitale. Di conseguenza, l'affermazione "Accedo con la mia firma" non è corretta.

I certificati di firma qualificata *non* possono essere impiegati da un soggetto per farsi riconoscere da un sistema.

- La firma digitale non è un grafo apposto in fondo ad un documento informatico.

La firma digitale è basata su un'operazione di cifratura che può aver operato solo il titolare del dispositivo di firma.

- L'acquisto di un dispositivo di autenticazione e firma non rappresenta l'abbonamento ad un servizio, ma l'acquisizione di uno strumento che consente di identificarsi laddove è richiesta l'autenticazione forte, e di sottoscrivere digitalmente documenti informatici.

- La firma digitale non è uno strumento per spedire documenti. Quindi è scorretta l'espressione "spedisco con la mia firma" e il titolare di una casella PEC non necessita di un dispositivo di firma.

Non devono trarre in inganno il fatto che i sistemi PEC fanno uso della firma digitale per sottoscrivere le ricevute, né il fatto che per accedere alla propria casella PEC-PCT è richiesto l'uso di un dispositivo di autenticazione.

- L'acquisizione di una casella di posta certificata non è equiparabile ad un'ipotetica certificazione di qualità di una casella e-mail ordinaria. La PEC è un sistema a sé stante e il termine "certificata" si riferisce alla peculiarità della PEC di *certificare* l'avvenuta spedizione e consegna (o mancata consegna) del messaggio e dell'eventuale documentazione allegata, la provenienza e l'integrità della comunicazione e gli orari di invio e di ricezione.

Se si è titolari del dominio della propria casella e-mail ordinaria, si può chiedere ad un gestore di PEC di accreditare il dominio sul sistema di posta certificata (ma è preferibile richiedere l'accreditamento di un sottodominio che include l'acronimo "pec"; per maggiori dettagli, vedere il quesito n. 11 del capitolo 7).

## 5.3 La dematerializzazione

La *dematerializzazione* è il processo mediante il quale gli atti transazionali (compravendite, incassi, pagamenti, assunzione o assolvimento di obbligazioni, ecc.) tra due o più soggetti e, in generale, quelli riguardanti la formazione di documenti rilevanti sotto il profilo giuridico, si realizzano senza altro supporto che quello informatico e/o telematico per l'acquisizione degli elementi costitutivi, l'elaborazione, l'archiviazione, il trasporto e la conservazione, con pieno valore tra le parti e verso i terzi (fonte Wikipedia).

La seguente tabella comparativa mira ad illustrare gli effetti della dematerializzazione sulle attività quotidiane dell'Avvocato. Il **carattere blu** evidenzia le parti che ricadono nel Processo Civile Telematico.

<b>TABELLA DI CORRISPONDENZA PER L'ATTUAZIONE DELLA DEMATERIALIZZAZIONE</b>	
<b>Sistema cartaceo</b>	<b>Sistema informatico e telematico (dematerializzato)</b>
<b>Documenti</b>	
Documento cartaceo	Documento informatico
Penna	Dispositivo di firma <sup>3</sup>
Documento cartaceo sottoscritto con firma autografa	Documento informatico corredato di impronta del documento sottoscritto digitalmente e di certificato di firma digitale del firmatario
<b>Strumenti per veicolare documenti</b>	
Posta ordinaria	Posta Elettronica Ordinaria (e-mail)
Posta raccomandata	Posta Elettronica Certificata (PEC, <a href="#">PEC-PCT</a> <sup>5</sup> )
<b>Luoghi</b>	
<ul style="list-style-type: none"> <li>• Domicilio legale del Professionista</li> <li>• Sede legale dell'Azienda</li> <li>• Sede legale dell'Ente Pubblico</li> </ul>	<ul style="list-style-type: none"> <li>• Casella di Posta Elettronica Certificata (Casella PEC)</li> <li>• <a href="#">Casella di Posta Elettronica Certificata per il Processo Telematico (CPECPT)</a><sup>5</sup></li> </ul>
Uffici Pubblici di un Ente	Sito internet dell'Ente Pubblico
Archivio cartaceo	Archivio informatico, conservazione sostitutiva <sup>7</sup>
<b>Strumenti di identificazione</b>	
Documento di identità	<ul style="list-style-type: none"> <li>• Nome utente e password (autenticazione debole<sup>1</sup>)</li> <li>• Carta Nazionale dei Servizi<sup>2</sup> (autenticazione forte<sup>1</sup>)</li> </ul>
<b>Strumenti di pagamento</b>	
Banconote, assegni, bancomat, carta di credito	Sistemi di pagamento on-line
<b>Azioni</b>	
Recarsi in un Ufficio Pubblico per: <ul style="list-style-type: none"> <li>• chiedere informazioni di carattere generale</li> <li>• reperire modulistica cartacea</li> </ul>	Accedere al sito internet dell'Ente Pubblico per: <ul style="list-style-type: none"> <li>• consultare le informazioni di pubblico accesso</li> <li>• scaricare modulistica informatica</li> </ul>
Recarsi in un Ufficio Pubblico e, previa identificazione: <ul style="list-style-type: none"> <li>• chiedere informazioni di propria pertinenza</li> <li>• ritirare copie di documenti cartacei</li> <li>• prenotare copie di documenti</li> <li>• depositare istanze e documenti cartacei sottoscritti con firma autografa</li> </ul>	Accedere al sito internet dell'Ente Pubblico e, previa autenticazione: <ul style="list-style-type: none"> <li>• consultare dati di propria pertinenza (<a href="#">Polisweb Nazionale</a>, <a href="#">JPolisweb</a><sup>6</sup>)</li> <li>• scaricare copie di documenti informatici (<a href="#">JPolisweb</a><sup>6</sup>)</li> <li>• richiedere la ricezione di copie di documenti nella propria casella PEC (<a href="#">JPolisweb</a><sup>6</sup>)</li> <li>• depositare istanze e documenti informatici sottoscritti con firma digitale (<a href="#">tramite PdA</a><sup>4</sup>)</li> </ul>
Spedire istanze e documenti cartacei via <ul style="list-style-type: none"> <li>• posta ordinaria</li> <li>• posta raccomandata</li> </ul>	Spedire istanze e documenti informatici via <ul style="list-style-type: none"> <li>• e-mail</li> <li>• PEC, <a href="#">PEC-PCT</a><sup>5</sup></li> </ul>
Aprire la propria cassetta postale con la chiave e: <ul style="list-style-type: none"> <li>• visionare la posta ricevuta</li> <li>• prelevare la posta ricevuta</li> </ul>	Accedere alle proprie casella di posta elettronica con autenticazione debole (PEC, e-mail) o <b>forte</b> ( <a href="#">PEC-PCT</a> <sup>5</sup> ) e: <ul style="list-style-type: none"> <li>• visionare la posta ricevuta (webmail o <a href="#">PdA</a><sup>4</sup>)</li> <li>• scaricare la posta sul proprio computer tramite un programma di posta elettronica (Outlook, Thunderbird...) o un gestionale di studio</li> </ul>

Tabella 3 - Tabella di corrispondenza per l'attuazione della dematerializzazione

- <sup>1</sup> **Autenticazione forte:** è basata sulla combinazione di più metodi di autenticazione, ad esempio oltre alla conoscenza di una password il possesso di qualcosa. L'autenticazione tramite smart card è forte in quanto basata sulla conoscenza del PIN e sul possesso del dispositivo.
- <sup>2</sup> **Carta Nazionale dei Servizi (CNS):** tessera (smart card) di formato ridotto con certificato digitale di autenticazione a bordo (insieme alla relativa chiave privata) rilasciata da una Pubblica Amministrazione e progettata per consentire al titolare l'accesso ai servizi telematici erogati da tutte le PA.
- <sup>3</sup> **Dispositivo di firma:** l'insieme dell'hardware e del software che consentono la sottoscrizione con firma digitale. Tipicamente è costituito da una tessera (smart card) di formato ridotto con a bordo il certificato di firma digitale (insieme alla relativa chiave privata), dal lettore necessario per collegare la tessera ad un computer, e dal software che rende possibile l'accesso alla smart card e l'uso del dispositivo.
- <sup>4</sup> **Punto d'Accesso al Processo Telematico (PdA):** cfr. capitolo 8.
- <sup>5</sup> **PEC-PCT, CPECPT:** cfr. capitolo 7, quesiti 14 e 15.
- <sup>6</sup> **Polisweb Nazionale:** consultazione tramite PdA di una copia centralizzata dei registri di cancelleria, aggiornata nottetempo dai singoli Uffici Giudiziari. La consultazione è limitata ai fascicoli di pertinenza dell'utente autenticato.  
**JPolisweb:** consultazione diretta dei fascicoli informatici di propria pertinenza tramite PdA, con possibilità di scaricare i documenti del fascicolo e richiederne le copie conformi.
- <sup>7</sup> **Conservazione sostitutiva:** procedura legale/informatica regolamentata dalla legge italiana, in grado di garantire nel tempo la validità legale di un documento informatico (fonte Wikipedia).



## 6 Servizi di consultazione

I servizi telematici attualmente più diffusi sono dati dai sistemi di consultazione. La consultazione di informazioni private è solitamente preceduta da una fase di autenticazione.

Eccone alcuni a titolo esemplificativo:

### **Polisweb**

Servizio telematico che consente agli utenti abilitati di consultare le informazioni principali, gli eventi e le scadenze relativi ai fascicoli del contenzioso e della volontaria giurisdizione per i quali l'utente collegato è costituito.

*Principali funzioni di consultazione del Polisweb:*

- **Agenda avvocato**

Consente di visionare, per i fascicoli per i quali l'avvocato connesso è costituito, gli eventi processuali registrati nel sistema informatico delle cancellerie in un determinato periodo di tempo (specificato dall'utente), raggruppati per fascicolo.

- **Fascicoli personali**

Consente di visualizzare le informazioni principali, gli eventi e le scadenze relative ad uno specifico procedimento (individuato dall'utente tramite l'apposita maschera di ricerca), per il quale l'avvocato connesso è costituito.

- **Archivio fascicoli**

Consente di visualizzare numero di ruolo e giudice relativi ad un procedimento per il quale l'avvocato collegato non è ancora costituito. E' necessario indicare l'esatta denominazione delle parti e la data dell'udienza, come indicata nell'atto di citazione.

Nella versione per il Processo Telematico (**JPolisweb**) consente di accedere direttamente al fascicolo informatico (e non a una copia dei dati di registro del fascicolo esportata nottetempo), di scaricare i documenti in esso contenuti, se disponibili, e di richiederne le copie conformi telematicamente.

### **Giudice di Pace**

Servizio con accesso libero (non richiede autenticazione) che consente a tutti, cittadini e avvocati, di attingere informazioni sullo stato dei procedimenti proposti innanzi al giudice di pace.

Il servizio consente anche di compilare online un ricorso in opposizione a sanzione amministrativa e la relativa nota di iscrizione a ruolo. E' possibile compilare anche la sola nota di iscrizione a ruolo.

### **Corte di Cassazione**

Servizio di consultazione dei Registri di Cancelleria Civile e Penale della Corte di Cassazione. E' richiesta l'autenticazione tramite smart card, a seguito della quale vengono resi disponibili i dati sui procedimenti di cui si è titolari.

### **Giustizia Amministrativa**

Servizio consente di consultare lo stato dei ricorsi al TAR.

La consultazione è ad accesso libero, e rende disponibile lo stato del ricorso a fronte dell'inserimento del numero di ruolo generale del ricorso stesso. In aggiunta, esiste un'area riservata che, previa autenticazione tramite smart card, consente di consultare lo stato di tutti i ricorsi associati al proprio codice fiscale.

Il servizio è gratuito, ma l'attivazione richiede la compilazione e l'invio, via fax, di un apposito modulo di adesione al servizio.

### **Gratuito Patrocinio**

Servizio predisposto dall'Ordine, che consente di visionare lo stato dell'istanza depositata presso l'Ordine stesso.

## 7 La Posta Elettronica Certificata (PEC)

La PEC è un sistema di posta elettronica che fornisce prova opponibile dell'invio e della consegna di un documento informatico. Il sistema PEC "certifica" anche la provenienza e l'integrità del messaggio, oltre che gli orari di invio e di ricezione del messaggio stesso.

Rimandando al sito del DigitPA (ex CNIPA) per gli approfondimenti normativi ([http://www.cnipa.gov.it/site/it-IT/Attività/Posta\\_Elettronica\\_Certificata\\_\(PEC\)/](http://www.cnipa.gov.it/site/it-IT/Attività/Posta_Elettronica_Certificata_(PEC)/)), passiamo in rassegna le questioni maggiormente riscontrate.

### **1) Quali sono i miei obblighi rispetto ai messaggi pervenuti nella casella PEC?**

Le comunicazioni tra cittadini, pubbliche amministrazioni, professionisti e imprese possono avvenire tramite PEC senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo (cfr. Legge 2/2009, art. 16, comma 9).

La comunicazione dell'indirizzo di PEC al proprio ordine di appartenenza da parte di un professionista può essere vista come l'elezione del proprio domicilio legale telematico, e ciascun professionista deve avere cura di **consultare costantemente e frequentemente la propria casella PEC** al fine di accertare la presenza di messaggi ricevuti, tenendo presente che nel sistema PEC, **il riferimento per i termini di decorrenza è il momento in cui il messaggio viene recapitato nella casella del destinatario.**

Per facilitare questo compito, i gestori offrono servizi di notifica dell'arrivo di messaggi PEC su caselle e-mail ordinarie o sul telefono cellulare (via SMS).

### **2) Adesso che ho una casella PEC, non conviene dismettere la casella di posta elettronica ordinaria?**

Conviene mantenere entrambe le caselle. **L'e-mail ordinaria continua ad essere uno strumento più pratico**, rispetto alla PEC, **per le comunicazioni che non richiedono una prova inoppugnabile dell'invio e della consegna.** Infatti, occorre considerare che ad ogni invio di un messaggio PEC, pervengono le ricevute (di accettazione da parte del proprio provider e, nel caso di destinatario PEC, di consegna o mancata consegna da parte del provider destinatario), che rappresentano un ingombro inutile per molte delle comunicazioni eseguite quotidianamente via e-mail. Inoltre il messaggio PEC non è di immediata lettura per il destinatario, in quanto non è riportato nel corpo della e-mail, ma in un allegato (nel sistema PEC il messaggio originale viene inserito all'interno di una "busta di trasporto").

Per fare un paragone con il cartaceo, è poco pratico usare la posta raccomandata per ogni missiva. In genere si utilizza la posta ordinaria, e si ricorre alla raccomandata solo quando si ritiene opportuno o necessario disporre di una prova inoppugnabile della consegna.

### **3) Ma essere titolare di più caselle comporta l'onere di consultarle tutte frequentemente!**

E' vero. Ma è anche vero che **i programmi di posta elettronica possono essere configurati per gestire più caselle.** Inoltre, è possibile (ed opportuno) impostare dei **filtri** che spostino i messaggi in una cartella separata, quando l'indirizzo di destinazione è quello PEC.

### **4) Non rischio di perdere le comunicazioni importanti in mezzo alla posta indesiderata (spam)?**

Il Garante della privacy afferma che la posta elettronica deve avere la stessa tutela di quella ordinaria ed è considerato illegale l'uso degli indirizzi e-mail per scopi diversi da quelli per cui sono presenti on-line (compreso l'invio di messaggi a scopo commerciale, pubblicitario...).

Rispetto al sistema e-mail ordinario, **nel sistema PEC c'è la certezza del mittente, che rappresenta un notevole deterrente per chi abusa della posta elettronica.** Chi invia posta indesiderata, può essere facilmente identificato e denunciato.

**Conviene, quindi, mantenere l'impostazione predefinita che respinge i messaggi provenienti da indirizzi non PEC, o impostarne la redirectione verso una casella e-mail ordinaria.**

Inoltre, i gestori di posta elettronica certificata effettuano un monitoraggio costante dell'uso dei domini di posta elettronica certificata e dispongono di strumenti di intervento tempestivo per prevenire gli abusi e rimuovere eventuali ostacoli al corretto funzionamento.

Ovviamente il problema si ripropone se si configura un programma di posta elettronica per ricevere i messaggi di tutte le caselle di cui si è titolari (PEC e non), ma è facilmente superabile, impostando dei filtri che spostino i messaggi in una cartella separata quando l'indirizzo di destinazione è quello PEC.

### **5) Devo preoccuparmi del possibile intasamento della mia casella PEC?**

**I gestori notificano l'avvicinarsi dell'esaurimento dello spazio disponibile** per la casella PEC.

**In ogni caso, esaurire lo spazio di 1 GB non è così immediato.** Si consideri che la Posta Certificata è poco trafficata: per le comunicazioni ordinarie si continuerà ad usare l'e-mail ordinaria; inoltre, la posta certificata è poco soggetta all'invio di posta indesiderata e abusi. In aggiunta, i documenti informatici di solito hanno dimensioni molto piccole rispetto allo spazio disponibile nella casella (considerando una dimensione tipica di un messaggio di 100 kB, una casella da 1 GB ne può contenere 10.000), ed esiste comunque un limite per la dimensione di un messaggio pari a 30 MB.

**E' importante, dal punto di vista dello spazio occupato, mantenere l'impostazione predefinita che respinge i messaggi provenienti da indirizzi non PEC, o impostarne la redirezione verso una casella e-mail ordinaria.**

Si noti che nel caso di impossibilità della consegna di un messaggio, anche nel caso in analisi (esaurimento dello spazio disponibile), è prevista l'emissione di una **ricevuta di mancata consegna**.

Per completare il quadro dei casi di mancata consegna, nel caso in cui non pervengano tutte le ricevute previste dal gestore del destinatario entro le dodici ore successive all'inoltro del messaggio, viene spedito al mittente un avviso di mancata consegna per superamento dei tempi massimi (ed esistono successivi step, per i quali si rimanda alla normativa).

### **6) Devo preoccuparmi dell'affidabilità dei gestori di PEC?**

**I gestori di PEC sono tutti tenuti a rispettare elevati requisiti di qualità e continuità del servizio e di sicurezza**, e sono sottoposti ai controlli del DigitPA (ex CNIPA). Inoltre i sistemi PEC sono soggetti a test di **interoperabilità**, volti a verificare che due utenti appartenenti a gestori diversi possano scambiarsi messaggi di posta certificata con le stesse garanzie di due utenti appartenenti allo stesso gestore.

Ovvero, i gestori di PEC **sono praticamente affidabili tutti allo stesso modo** e sono spesso ingiustificate marcate differenze sul canone della casella, a parità di servizi offerti.

### **7) E' possibile spedire da una casella e-mail ordinaria a una casella PEC, o viceversa?**

E' sempre possibile spedire da una casella PEC a una casella e-mail ordinaria. Inoltre è possibile configurare la propria casella PEC per ricevere messaggi da caselle e-mail ordinarie, ma **non conviene, onde evitare la ricezione di posta indesiderata nella casella PEC**.

Si consideri che **lo scambio di documenti ha pieno valore legale solo se avviene fra caselle PEC**.

D'altra parte la comunicazione da PEC verso caselle ordinarie può essere usata per l'inoltro di **comunicazioni che necessitano dell'attestazione dell'invio, ma non richiedano la certificazione della consegna** (ad esempio l'invio di fatture).

### **8) Come faccio a sapere se un'ente pubblico dispone di una casella PEC?**

E' disponibile un registro elettronico delle Pubbliche Amministrazioni all'indirizzo [www.indicepa.gov.it](http://www.indicepa.gov.it)

**Le PA sono tenute a istituire una casella di posta certificata per ciascun registro di protocollo** e a comunicarlo al DigitPA (ex CNIPA), che provvede a pubblicare l'indirizzo PEC nel suddetto registro informatico.

### 9) Ho sentito dire che le ricevute di consegna della PEC perdono validità col tempo.

Gli algoritmi e lunghezze di chiavi attualmente in uso dovrebbero garantire per **almeno una decina di anni** l'impossibilità di risalire alla chiave privata con cui è stato firmato un documento informatico.

**Per garantire la validità legale di un documento informatico nel tempo** è prevista la **conservazione sostitutiva** ([http://it.wikipedia.org/wiki/Conservazione\\_sostitutiva](http://it.wikipedia.org/wiki/Conservazione_sostitutiva)).

### 10) Come posso gestire l'archiviazione dei messaggi e delle ricevute?

La PEC è un sistema di trasmissione di documenti. La norma che impone ai **gestori** il mantenimento di un **registro informatico delle operazioni svolte negli ultimi trenta mesi che consente la riproduzione delle ricevute, con lo stesso valore giuridico**, non deve indurre a considerare i gestori incaricati dell'archiviazione dei dati dei titolari delle caselle. Come nel sistema postale cartaceo, l'archiviazione e la conservazione dei documenti spediti e ricevuti sono a cura del titolare della casella.

**Fermo restando che per preservare la validità nel tempo dei documenti informatici sottoscritti digitalmente**, incluse le ricevute della PEC, è prevista la **conservazione sostitutiva** ([http://it.wikipedia.org/wiki/Conservazione\\_sostitutiva](http://it.wikipedia.org/wiki/Conservazione_sostitutiva)), **è ragionevole che l'utente avverta come più immediata esigenza di preservarsi semplicemente dalla perdita accidentale delle ricevute (ad esempio, per un danno al disco fisso o per erronea cancellazione).**

Sono possibili varie **soluzioni**, anche sovrapponibili:

- è sempre raccomandabile il tradizionale backup giornaliero del sistema, che consente di ripristinarlo in caso di guasto, possibilmente in combinazione con l'adozione di un sistema di mirroring del disco fisso (salvataggio in tempo reale dei dati su due dischi, in modo da non pregiudicare la funzionalità del sistema, con danno per la propria attività professionale, a causa del guasto del disco fisso);
- è possibile configurare il proprio programma di posta elettronica in modo che i messaggi, una volta scaricati, non vengano cancellati dal server del gestore; tuttavia, occorre tenere presente la conseguente occupazione di spazio sulla casella;
- i gestori di PEC in genere offrono un servizio denominato "Archivio di Sicurezza", ovvero uno spazio su disco sui loro sistemi dedicato all'archiviazione di una copia di ogni messaggio.

### 11) Come faccio a distinguere gli indirizzi di posta elettronica ordinaria da quelli di posta certificata?

Purtroppo non è stata definita una normativa al riguardo (ad es. riservare ed imporre per i domini di posta certificata la presenza dell'acronimo "pec" o dell'abbreviazione "cert", separati dal resto del nome di dominio con un trattino o un punto).

E' opportuno che chi decide di far registrare un proprio dominio nel sistema PEC, registri un nome di dominio da cui si evinca immediatamente che si tratta di posta certificata (ad es. [pec.studiolegalebrambilla.it](http://pec.studiolegalebrambilla.it) o [studiolegalebrambilla-cert.it](http://studiolegalebrambilla-cert.it) (\*)).

Dal punto di vista pratico, c'è il riscontro al momento della spedizione: una volta inviato il messaggio, se l'indirizzo di destinazione è una PEC, deve pervenire la ricevuta di avvenuta o mancata consegna.

(\*) E' possibile chiedere ad un gestore di PEC di accreditare il proprio dominio [avvocatobrambilla.it](http://avvocatobrambilla.it) sul circuito di posta certificata, ma ciò non può praticamente essere fatto per le caselle e-mail fornite diffusamente dai vari provider (ad es. libero.it, tiscali.it, virgilio.it, yahoo.it), dal momento che significherebbe trasferire in blocco tutti gli utenti sul sistema PEC (!).

D'altra parte, anche il trasferimento del proprio dominio [avvocatobrambilla.it](http://avvocatobrambilla.it) sul sistema PEC non è una buona prassi, dal momento che non è possibile evincere se si tratta di un indirizzo PEC dalla lettura del solo dominio (la parte dell'indirizzo a destra della chiocciola @). E' opportuno, piuttosto, attestare sul sistema PEC un dominio di livello inferiore, ad es. [pec.avvocatobrambilla.it](http://pec.avvocatobrambilla.it), lasciando il dominio [avvocatobrambilla.it](http://avvocatobrambilla.it) sul sistema e-mail ordinario (oppure adottare un ulteriore dominio dedicato, dal nome del quale si evince subito che si tratta di una casella PEC, ad es. [avvocatobrambilla-cert.it](http://avvocatobrambilla-cert.it)).

### **12) La PEC certifica il mittente e il destinatario della comunicazione?**

Purtroppo le attuali procedure di accertamento dell'identità di un soggetto richiedente la casella di PEC non sono rigorose come quelle per il rilascio dei certificati di firma digitale (che richiedono l'autenticazione *de visu* del titolare) e, soprattutto, non sono riconducibili a regole di sicurezza comuni dettate dal Ministero, per cui in linea di principio è possibile il "furto d'identità" nella forma di acquisto, da parte di un malintenzionato, di una casella PEC fornendo le credenziali di un altro soggetto.

In questo contesto è certamente utile la verifica dell'identità dell'iscritto da parte degli ordini professionali al momento della comunicazione dell'indirizzo PEC ai sensi della legge 2/2009. Inoltre gli iscritti possono sempre verificare l'esattezza del proprio indirizzo PEC pubblicato sull'albo e anche i mittenti potranno segnalare indirizzi non validi, che potranno essere corretti tempestivamente. Quindi, **è ragionevole prevedere che gli elenchi mantenuti dagli ordini professionali, a regime, saranno affidabili.**

Analogamente, l'indice delle Pubbliche Amministrazioni mantenuto dal DigitPA (ex CNIPA) può essere considerato ragionevolmente affidabile.

Chi dispone di un **dispositivo di autenticazione**, può configurare il proprio programma di posta elettronica per l'invio di messaggi S/MIME, in modo da garantire ulteriormente l'identità del mittente e l'integrità del messaggio inviato.

### **13) E' vero che inviando dati sensibili via PEC si viola il segreto professionale?**

I dati dei sistemi PEC attraversano le reti di interconnessione su canali cifrati, ma **sono potenzialmente disponibili in chiaro presso i gestori mittenti e destinatari.**

Di fronte a questa preoccupazione, è utile far presente che questa potenziale disponibilità dei dati esiste **anche con la posta elettronica ordinaria** che, rispetto alla PEC, transita in chiaro anche sulle reti di interconnessione.

Certamente, il sistema PEC fornisce maggiori garanzie rispetto alla posta elettronica ordinaria anche per il trattamento dei dati, in quanto i gestori di PEC, oltre a dover garantire il rispetto delle misure di sicurezza previste dal codice per il trattamento dei dati personali, sono soggetti ad ulteriori vincoli, sotto la vigilanza del DigitPA (ex CNIPA). Ad esempio, i gestori di PEC devono possedere gli stessi **requisiti di onorabilità** richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche, devono dimostrare l'affidabilità organizzativa e tecnica necessaria per svolgere il servizio ed impiegare personale dotato di conoscenze ed esperienza specifiche.

**E' comunque possibile garantirsi la riservatezza di una comunicazione verso un singolo destinatario anche rispetto ai gestori, operando la cifratura del messaggio inviato**, ma occorre disporre della chiave pubblica del destinatario e importarla nel proprio programma di posta elettronica.

### **14) Ho già una casella PEC-PCT. A cosa mi serve un'altra casella di Posta Elettronica Certificata?**

La casella di PEC-PCT è usata specificatamente per le comunicazioni a valore legale nell'ambito della giustizia civile, secondo le regole del Processo Civile Telematico. **Dal punto di vista dell'avvocato civilista, la PEC è un sistema di posta elettronica certificata complementare rispetto alla PEC-PCT**, utilizzabile per le comunicazioni a valore legale con le Pubbliche Amministrazioni o con altri soggetti provvisti di casella PEC al di fuori della giustizia civile.

La casella PEC-PCT viene rilasciata tramite iscrizione al cosiddetto *Punto d'Accesso al Processo Telematico* ed è accessibile previa autenticazione forte con Carta Nazionale dei Servizi su quest'ultimo.

Le disposizioni normative relative alla PEC non sono applicabili al Processo Civile Telematico, per esplicita esclusione operata dal D.P.R. 11 febbraio 2005, n. 68 il cui art. 16 stabilisce che "[...] *Le disposizioni di cui al presente regolamento non si applicano all'uso degli strumenti informatici e telematici nel processo civile, nel processo penale, nel processo amministrativo, nel processo tributario e nel processo dinanzi alle sezioni giurisdizionali della Corte dei Conti, per i quali restano ferme le specifiche disposizioni normative*".

Tuttavia sono già state varate delle leggi che prevedono l'uso della PEC nell'ambito del processo penale e nei mesi scorsi, alcuni esponenti del Ministero hanno più volte manifestato l'intenzione di estendere l'uso

della PEC alle comunicazioni nel contenzioso civile e dismettere, di conseguenza, la PEC-PCT. Ma non sono ancora stati divulgati né un regolamento, né un piano tecnico per realizzare questo cambiamento.

### **15) Sento parlare di diverse tipologie di posta certificata, con vari acronimi. Rischio di confondermi...**

#### **e-mail**

Si tratta della posta elettronica ordinaria. Le comunicazioni e gli invii di documenti attraverso tale sistema non hanno pieno valore legale.

#### **PEC**

Posta Elettronica Certificata. E' uno strumento che permette l'invio di messaggi di posta elettronica che hanno lo stesso valore legale di una raccomandata con ricevuta di ritorno.

#### **CEC-PAC**

E' acronimo di "Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadino". Le caselle CEC-PAC vengono fornite gratuitamente da enti pubblici ai cittadini per favorire la dematerializzazione nelle comunicazioni fra i cittadini stessi e le PA. Si tratta, tecnicamente, di caselle di Posta Elettronica Certificata, ma consentono di comunicare con le sole PA, e non sono utilizzabili per comunicazioni fra privati, professionisti e imprese. Quindi il professionista non può comunicare una casella CEC-PAC al proprio ordine professionale ai sensi della Legge 2/2009.

E' verosimile che il rilascio di caselle PEC gratuite con uso limitato sia stato concepito per evitare che lo Stato si aggravi delle caselle dei professionisti e dei servizi annessi, e/o per evitare una situazione di monopolio da parte delle aziende appaltatrici della "PEC di Stato".

#### **PEC-PCT**

Sistema di Posta Elettronica Certificata dedicato alle comunicazioni a valore legale nell'ambito del contenzioso civile.

#### **CPECPT**

E' acronimo di "Casella di Posta Elettronica Certificata del Processo Telematico". Originariamente la Casella PEC-PCT veniva indicata con quest'acronimo, tuttora presente nelle Regole Tecniche per il Processo Civile Telematico attualmente in vigore (D.M. 17 Luglio 2008).

#### **Posta S/MIME**

Sistema di posta elettronica con firma digitale del messaggio da parte del mittente. Nei sistema S/MIME non possono essere adoperati i certificati di firma qualificata, in quanto dedicati alla sottoscrizione dei documenti informatici. In compenso, i certificati di autenticazione in genere sono abilitati per la firma delle e-mail.

Isistemi del Processo Civile Telematico fanno uso di posta S/MIME: l'invio di documenti agli Uffici Giudiziari (imbustati conformemente alle Regole Tecniche per il Processo Civile Telematico, con l'ausilio di appositi software) non avviene tramite PEC-PCT, ma con un messaggio S/MIME sottoscritto dal Punto d'Accesso al Processo Telematico (PdA).

## 8 Il Punto d'Accesso al Processo Telematico (PdA)

Sistema esposto su internet che, attualmente, include i seguenti servizi.

1) Attribuzione al professionista di una **Casella PEC-PCT** (o CPECPT). Le Regole Tecniche del Processo Civile Telematico prevedono che la casella PEC-PCT venga rilasciata da un PdA previa iscrizione.

Rispetto alla PEC, la PEC-PCT:

- non può essere usata con un comune programma di posta elettronica, piuttosto richiede l'accesso al PdA, con autenticazione forte (tramite CNS);
- i documenti informatici devono essere imbustati secondo le Regole Tecniche del Processo Civile Telematico, facendo uso di appositi software;
- è il sistema di posta certificata *ad hoc* per la giustizia civile (i biglietti di cancelleria del processo civile vengono recapitati nelle caselle PEC-PCT, ed è previsto che l'invio delle copie conformi dall'Ufficio Giudiziario e delle notifiche tra difensori avvengano via PEC-PCT).

Nei mesi scorsi alcuni esponenti del Ministero di Giustizia hanno più volte manifestato l'intenzione di estendere l'uso della PEC alle comunicazioni nel contenzioso civile e dismettere, di conseguenza, la PEC-PCT. Ma non sono ancora stati divulgati né un regolamento, né un piano tecnico per realizzare questo cambiamento.

2) La possibilità di **depositare atti** (attualmente limitata ai ricorsi per ingiunzione, ma che a breve verrà estesa alle procedure esecutive e concorsuali, alle memorie e a tutti i tipi di atti, man mano che i tribunali si predisporranno per gestirli telematicamente) e **inoltrare notifiche** alla controparte.

Gli atti e le notifiche devono essere imbustati conformemente alle Regole Tecniche per il Processo Civile Telematico, facendo uso di appositi software.

3) L'accesso ai sistemi di consultazione dei registri delle cancellerie civile, denominati **Polisweb**, limitatamente ai fascicoli di propria pertinenza.

Il Polisweb, allo stato, prevalentemente rende disponibile una copia dei dati di registro dei fascicoli, ma a regime prevede la consultazione diretta del fascicolo informatico e dei documenti in esso inclusi. L'interazione diretta con l'ufficio giudiziario consentirà anche la richiesta delle copie conformi dei documenti per via telematica, di provvedere al pagamento telematico delle stesse e di riceverle nella casella PEC-PCT.