Il Processo Civile Telematico

di Maurizio Reale

Supplemento Altalex Quotidiano - Gennaio 2014

IL PROCESSO CIVILE TELEMATICO
di Maurizio Reale

Sommario

Prefazione

Nel mondo giuridico ed in particolare in quello forense, il significato delle più elementari nozioni dell'informatica giuridica quali, ad esempio, il significato delle parole PEC, CPECPT, P.D.A., sono quasi sempre confuse dalla maggior parte di coloro che, oramai, con il processo telematico devono interagire se vogliono continuare ad esercitare la professione legale.
La prova di tale "ignoranza informatica" può essere facilmente verificata tramite la consultazione dei più famosi motori di ricerca nei quali inserendo, ad esempio, la frase "processo telematico" riceviamo a riscontro molte pagine web ma poche (veramente poche) sono quelle che da una parte affrontano tecnicamente l'argomento e, dall'altra contengono informazioni aggiornate. Anche in Facebook, uno dei più frequentati social network, troviamo pochissime pagine sull'argomento e le stesse non vengono molto frequentate dagli utenti.
Una nota critica non può non essere rivolta anche ai Consigli dell'Ordine che, a mio avviso, non hanno dedicato e non dedicano al processo telematico la giusta attenzione organizzando, ad esempio, eventi formativi che stimolino la curiosità degli iscritti; è palese come, a livello nazionale, la percentuale di eventi a tema "processo civile telematico" è veramente bassa se paragonata a quelli relative alle altre discipline. Tale "pigrizia" appare ancora più grave considerando che il 30 giugno 2014 entrerà in vigore l'esclusività (obbligo) del deposito telematico di atti e documenti in tutti i Tribunali italiani.
Obiettivo del presente lavoro è quindi quello di avvicinare i colleghi ad una conoscenza di base del processo telematico che possa facilitarne la conoscenza e l'utilizzo anche e soprattutto per essere pronti ad affrontare, con serenità o con meno paure, la data del 30 giugno 2014.

Capitolo I
Le origini del P.C.T.

Sommario: Premessa - 1.1. Le statistiche del P.C.T. – agosto 2013 - 1.1.1 Le statistiche del PCT - agosto 2013: il deposito di atti e documenti telematici a valore legale - 1.1.2 Le statistiche del PCT - agosto 2013: le comunicazioni telematiche a valore legale

Premessa

Il processo civile telematico (P.C.T.) nasce dalla esigenza di combinare le nuove tecnologie dell'informazione e della comunicazione con l'organizzazione giudiziaria e la norma processuale[1].
È possibile far risalire l'origine del processo telematico alle disposizioni della L. n. 59/1997 che, con l'articolo 15, attribuisce ai documenti informatici, agli atti ed ai dati della Pubblica Amministrazione, formati sui supporti informatici o trasmessi per via telematica, valore e rilevanza ad ogni effetto di legge; con il DPR n. 513/1997 viene poi introdotta nel nostro ordinamento la firma digitale[2].
Il primo vero intervento normativo del legislatore è però del 13 febbraio 2001 con il D.P.R. n. 123 dalla cui lettura è possibile desumere come, con l'utilizzo del mezzo informatico nel processo, si sia cercato di facilitare il risparmio di energie materiali e personali e la funzionalità dell'intero sistema processuale il tutto nel tentativo di rendere più facile il lavoro non solo per il personale della Pubblica Amministrazione ma anche, e soprattutto, per gli avvocati e per tutti i cittadini.
Il P.C.T. doveva superare una fase di sperimentazione fissata inizialmente per settembre 2004, poi rimandata a settembre 2005 ed infine svolta nel 2006.
I Tribunali di Genova e Milano sono stati i primi a passare dalla fase teorica a quella pratica dell'utilizzo del P.C.T. e ciò avveniva nel corso dell'anno 2006; in particolare l'11 dicembre 2006 la sperimentazione veniva conclusa e il Tribunale di Milano poteva così beneficiare dell'attivazione del decreto ingiuntivo telematico ove, inizialmente erano coinvolti circa 300 avvocati, 30 magistrati e 15 cancellieri mentre, alla data del 30 maggio 2007, erano circa 1.300 i decreti ingiuntivi telematici gestiti con una media quindi di 15-20 depositi giornalieri[3].

1.1. Le statistiche del P.C.T. (rilevazione agosto 2013)

Le statistiche ufficiali del Ministero della Giustizia così come pubblicate sul sito dedicato al processo civile telematico[4] sono indicative di come dal secondo semestre del 2011 si siano registrati indiscutibili progressi nell'avanzamento del programma di informatizzazione della giustizia civile italiana.
Il sistema SIECIC per le esecuzioni civili individuali e concorsuali è attivo in tutti i 26 Distretti e, conseguentemente, funzionante in 164 su 165 Tribunali italiani.

---

[1] S. BRESCIA P. LICCARDO, *Enciclopedia Giuridica*, voce *Processo telematico*, Volume aggiornamento XIV, 2006 Istituto della Enciclopedia Italiana Treccani spa.

[2] GIANNI BUONOMO, *Il processo telematico nella degenerazione delle tecniche legislative*, in www.interlex.it il, 31 maggio 2005.

[3] Il decreto ingiuntivo telematico: innovazione tecnologica, normativa, sociale organizzativa. L'esperienza del Tribunale di Milano – nota della dott.ssa Amelia Torrice, resp. Ufficio Sistemi Informativi Automatizzati per la giustizia civile e il processo civile telematico della D.G.S.I.A.

[4] http://pst.giustizia.it/PST/resources/cms/documents/DgsiaStatoProgettiLug13.pdf

Il sistema SICID per la cognizione civile (comprensivo del lavoro e della volontaria giurisdizione) è attivo in tutte le Corti d'Appello ed in tutti i Tribunali.
Con l'installazione dei registri sopra citati è stato possibile attivare i servizi telematici che consentono di mettere a disposizione dell'avvocatura, i dati contenuti nei registri di cancelleria del processo di cognizione e di esecuzione (cd. Polisweb / SICID e Polisweb / SIECIC). In particolare: per il processo di cognizione il servizio risulta attivato in 174 uffici giudiziari e più precisamente in 28 Corti d'Appello e in 165 Tribunali; per il processo esecutivo il servizio è attivo in 164 Tribunali su 165. Tale sistema consente agli avvocati di consultare online il fascicolo digitale che raccoglie gli atti ed i documenti del processo; ciò significa che il professionista potrà consultare, memorizzare sul proprio pc e stampare ogni singolo atto inserito nel fascicolo direttamente dal proprio studio senza doversi recare fisicamente allo sportello della cancelleria.
Inoltre è stato istituito su tutto il territorio nazionale il sistema per la consultazione online dei procedimenti trattati dagli uffici dei Giudici di Pace.

1.1.1 Le statistiche del P.C.T. – agosto 2013: il deposito di atti e documenti telematici a valore legale

La vera e propria svolta però si è avuta con la possibilità di depositare atti e documenti telematici firmati digitalmente, cosa questa che consente il deposito telematico di documenti informatici a valore legale, firmati digitalmente e trasmessi (su canali sicuri autenticati e criptati) tramite punto d'accesso al Gestore Centrale e da questi alla Cancelleria competente tramite il Gestore Locale.
Ciò significa che l'avvocato per il deposito del proprio atto (memoria, nota spese, comparsa conclusionale, comparsa di costituzione e risposta ecc. ecc.) non dovrà più recarsi fisicamente in Cancelleria per effettuare manualmente il deposito ma potrà farlo telematicamente dal proprio studio inviando l'atto, firmato digitalmente, dal proprio p.c. sfruttando il collegamento internet.
Gli atti inviati dagli avvocati vengono quindi inseriti nel fascicolo informatico e, alimentando automaticamente i registri di cancelleria, consentono numerosi risparmi anche all'amministrazione:

- riduzione degli oneri di accesso agli uffici giudiziari
- riduzione dei costi inerenti la gestione cartacea dei procedimenti
- riduzione dei tempi di lavoro all'interno degli uffici giudiziari
- possibilità di recuperare personale amministrativo da dedicare ad altre attività di ufficio.

Il deposito telematico, al 5 agosto 2013, è attualmente attivo a valore legale in 7 Corti d'Appello su 28 in 91 Tribunali su 165 e, relativamente a questi ultimi, riguarda sia i procedimenti di ingiunzione, sia i procedimenti di esecuzione immobiliare, nonché il deposito delle memorie *ex* art. 183 c.p.c., comparse di costituzione, comparse conclusionali e atti dei giudici.
Gli atti giudiziari depositati telematicamente, con riferimento al periodo "luglio 2012 – luglio 2013", sono pari a 237.726[5].

1.1.2. Le statistiche del P.C.T. – agosto 2013: le comunicazioni telematiche a valore legale

Il servizio consiste nella automatica esecuzione delle comunicazioni di cancelleria agli avvocati in coincidenza con il verificarsi di alcuni eventi processualmente previsti e con l'aggiornamento del

[5] http://pst.giustizia.it/PST/resources/cms/documents/DgsiaStatoProgettiLug13.pdf

registro da parte della cancelleria, e prevede altresì l'inserimento automatico della ricevuta elettronica nel fascicolo informatico all'interno del quale è conservata a valore legale.
Dal 18 febbraio 2013 in tutti i Tribunali e Corti d'Appello vige il principio della esclusività della comunicazione telematica e ciò a seguito del decreto legge 179/2012 e della legge 228/2012.
Dal novembre 2011 (introduzione della PEC) sono state consegnate ben 14.600.000 comunicazioni telematiche.
L'esclusività dell'invio telematico della comunicazione di cancelleria, oltre a consentire risparmio di tempo e di operazioni per tutti gli operatori di giustizia, consente soprattutto un risparmio di costi; infatti, calcolando (prima della comunicazione telematica) un costo unitario medio di € 5,00 e moltiplicando tale costo per 12 milioni di comunicazioni all'anno risulta un risparmio annuo fino a 60 milioni di Euro e, pur volendo considerare che attualmente risulta che le comunicazioni di cancelleria vengono spedite anche per eventi che non ne prevedano l'obbligo, riducendo conseguentemente l'indicata somma del 30 / 40%, si ottiene comunque un risparmio annuo minimo non inferiore ai 35/40 milioni di Euro[6].

[6] http://pst.giustizia.it/PST/resources/cms/documents/DgsiaStatoProgettiLug13.pdf

Capitolo II
L'utilizzo del P.C.T.

Sommario: 2.1. Cosa è possibile fare con il P.C.T. - 2.2. Gli strumenti necessari per l'utilizzo del P.C.T. - 2.3. Chi può utilizzare il P.C.T.

2.1. Cosa è possibile fare con il P.C.T.

È da premettere, sul punto, che quanto di seguito indicato è possibile da realizzare in quanto i Tribunali abbiano o dato inizio alla sperimentazione o abbiano ricevuto dal Ministero della Giustizia il decreto che concede il valore legale alle seguenti attività:

- consultare via internet i propri fascicoli così come depositati nelle cancellerie di Giudici di Pace, Tribunali, Corti d'Appello e Corte di Cassazione tramite il POLISWEB;
- redigere e firmare tutti gli atti di parte;
- depositare gli atti di parte;
- ricevere tutte le comunicazioni da parte dell'Ufficio Giudiziario;
- richiedere il rilascio di copie di atti (servizio ancora non attivo);
- richiedere agli Uffici del Ruolo della Procura della Repubblica le informazioni ostensibili ex art. 335 c.p.p.;
- ricevere l'avviso ex art 415 bis c.p.p., richiedere e ricevere telematicamente la copia del fascicolo;
- richiedere e ricevere telematicamente le trascrizioni dei verbali delle udienze penali;
- pagare le spese di giustizia (contributo unificato e diritti di copia) attraverso i pagamenti telematici.

2.2. Gli strumenti necessari per l'utilizzo del P.C.T.

Per l'uso telematico del processo civile è necessario essere dotati di:

- computer con sistema operativo: Windows 98, 2000, XP, Vista, Seven, Mac OS X v. 10.4 o successiva, GNU/Linux Ubuntu;
- collegamento a internet (preferibilmente a banda larga);
- browser internet: Microsoft Internet Explorer (versione 6 o superiore, solo per Windows), Mozilla Firefox (per tutti i sistemi operativi), Google Chrome (solo per Windows), Apple Safari (per Mac e Windows);
- software antivirus, antispam e firewall (soprattutto a protezione della PEC);
- firma digitale: consigliata su business key (chiavetta USB) o, in alternativa smart card con lettore idoneo. La firma digitale ha la funzione di consentire la interazione online con i siti web che richiedono all'utente di identificarsi in maniera certa e conforme alle normative vigenti affinché lo stesso possa essere riconosciuto dal "sistema Giustizia" come soggetto abilitato al processo telematico;
- P.E.C. (posta elettronica certificata) con la quale l'utente può legalmente depositare e ricevere gli atti del processo e che a seguito del D.M. 21 febbraio 2011 n. 44 è diventata il mezzo di comunicazione ufficiale nel PCT;
- P.D.A. (punto di accesso al sistema Giustizia) che, a seguito delle nuove regole tecniche dettate dal D.M. 21 febbraio 2011, n. 44, può essere privato (messo a disposizione da privati autorizzati dal Ministero della Giustizia) o pubblico (per il tramite del Portale dei Servizi Telematici del dominio Giustizia).

Il P.D.A. (pubblico o privato) ha come funzione quella di riconoscere con certezza coloro che vogliono accedere al processo telematico controllando quindi la loro identità, il ruolo (avvocato o praticante abilitato), la possibilità di esercitare il loro ruolo verificando che il soggetto non sia sospeso, radiato, cancellato.
Prima dell'entrata in vigore del D.M. 21 febbraio 2011, n. 44 l'avvocato poteva essere iscritto ad un solo P.D.A.; con le nuove regole tecniche invece è possibile che lo stesso sia iscritto a più P.D.A. contemporaneamente.

2.3. Chi può utilizzare il P.C.T.

L'utilizzo del PCT è rivolto a :

- avvocati e praticanti abilitati al patrocinio iscritti all'Ordine. A questo proposito credo sia opportuno precisare che anche un professionista nel cui Distretto non sia ancora operativo il P.C.T. può comunque utilizzarlo in tutti gli altri Distretti in cui lo stesso sia operativo con valore legale;
- altri soggetti esterni che per la loro qualifica hanno titolo ad interagire con il P.C.T. (C.T.U. ecc.).

Capitolo III
La sperimentazione e il valore legale del processo telematico

Sommario: Premessa - 3.1. La sperimentazione del P.C.T. – 3.2. Il valore legale del P.C.T.

Premessa

Affinché ad un Tribunale possa essere riconosciuto il valore legale per il deposito telematico di atti e/o documenti è necessario porre in essere una serie di passaggi obbligatori.
Nella prima fase, che possiamo definire preliminare, la normativa prevede determinati adempimenti a carico sia dell'Ufficio Giudiziario sia del Consiglio dell'Ordine.
L'Ufficio Giudiziario, nello specifico, dovrà curare sia l'aspetto relativo all'hardware e al software, di cui dovranno essere dotati i computer delle cancellerie, sia quello della formazione del personale di cancelleria all'utilizzo della nuova tecnologia.
Il Consiglio dell'Ordine ha invece, a mio avviso, il maggior numero di oneri da assolvere in quanto:

- dovrà dotarsi di P.D.A. se vorrà garantire migliori servizi e migliori condizioni economiche agli iscritti per l'accesso e l'utilizzo del P.C.T;
- dovrà nominare un delegato per la firma digitale del documento di censimento da inviare a D.G.S.I.A., così come richiesto dalle nuove regole tecniche, il quale delegato dovrà curare poi l'invio dell'Albo telematico (firmato digitalmente) in formato XML al Ministero della Giustizia affinché i dati degli iscritti possano essere inseriti nel Registro Generale degli Indirizzi Elettronici (Re.G.Ind.E.);
- dovrà obbligatoriamente comunicare l'avvenuta cancellazione, radiazione, sospensione o modifica di uno dei dati presenti nell'anagrafica dell'iscritto entro le 72 ore successive dal verificarsi di uno degli eventi appena citati[7];
- dovrà reperire tra i propri iscritti coloro che daranno vita alla sperimentazione del processo telematico.

Ultimati questi adempimenti preliminari sarà possibile passare alla sperimentazione vera e propria.

3.1. La sperimentazione del P.C.T.

La **sperimentazione** è quella fase nella quale si accertano e testano l'installazione e l'idoneità delle attrezzature informatiche presso l'Ufficio Giudiziario unitamente alla funzionalità dei servizi di comunicazione dei documenti informatici.
Qui i protagonisti sono soprattutto gli avvocati sperimentatori i quali dovranno inviare telematicamente gli atti.
In questa fase (aperta anche ai non sperimentatori ufficiali) vige il **principio del doppio binario**: l'avvocato dovrà depositare il proprio atto prima in via telematica poi, affinché il deposito abbia valore legale, il giorno dopo dovrà provvedere a depositare lo stesso atto in forma cartacea.
Attenzione: solo il deposito del cartaceo, in regime del doppio binario, conferisce il valore legale all'attività dell'avvocato.

[7] http://www.processotelematico.giustizia.it/pdapublic/resources/PCT-Specifiche%20invio%20albi%20avvocati%20v1.4.pdf

3.2. Il valore legale del processo telematico

Accertato da parte del Ministero della Giustizia sia l'esito positivo della fase di sperimentazione sia l'installazione e l'idoneità delle attrezzature informatiche presso il Tribunale (unitamente alla funzionalità dei servizi di comunicazione dei documenti informatici), il Ministero stesso avrà cura di emanare un decreto nel quale verrà dichiarata l'attivazione del processo civile telematico presso il Tribunale a norma dell'art. 35, comma 1, D.M. 21 febbraio 2011, n. 44 relativamente ai documenti oggetto della sperimentazione conclusa con successo.
Credo sia opportuno precisare che l'emissione del decreto che attribuisce il valore legale del deposito telematico degli atti non equivale, fino al 29 giugno 2014, ad obbligo; ossia, l'avvocato potrà continuare a depositare il proprio atto in forma cartacea pur trovandosi in un Tribunale nel quale, per quel tipo di atto, il Ministero della Giustizia abbia emesso il valore legale per il deposito telematico.
Questo sarà consentito, come anticipato, fino al 29 giugno 2014 in quanto, dal 30 giugno 2014 entrerà in vigore la norma che prevede, **in tutti i Tribunali**, **l'esclusività del deposito telematico di atti e documenti.**
Sul punto rimando alla lettura del capitolo VI.

Capitolo IV
Le regole tecniche del processo telematico prima e dopo il D.M. 44/2011

Sommario: Premessa - 4.1. Il passaggio dalla C.P.E.C.P.T. alla P.E.C. - 4.1.1 La C.P.E.C.P.T. - 4.1.2 La PEC - 4.2. La natura e la funzione del P.D.A. prima e dopo il D.M. 21 febbraio 2011, n. 44 - Il Portale dei Servizi Telematici - 4.2.1. Funzioni del P.D.A. - 4.2.2. Impossibilità, per professionisti e Ordini, di essere iscritti a più P.D.A. contemporaneamente - 4.2.3. Il P.D.A. dopo il D.M. 21 febbraio 2011, n. 44 - 4.2.4. Il momento del passaggio dal vecchio al nuovo P.D.A. e dalla CPECPT alla PEC - 4.2.5. Il Portale dei Servizi Telematici e l'utilità del P.D.A. dopo il D.M. 21 febbraio 2011, n. 44. - 4.2.5. Nuove regole tecniche e adempimenti del C.O.A. - 4.2.6. Processo Telematico e Cloud Computing

Premessa

A distanza di dieci anni dal primo provvedimento normativo specifico (D.P.R. n. 123/2001) vengono emanate, il 22 febbraio 2011, con il D.M. n. 44 le nuove regole tecniche del processo telematico e, il 18 luglio 2011 le specifiche tecniche previste dall'art. 34 del citato decreto.
È possibile affermare che le modiche apportate rappresentano (come già detto in premessa) una vera e propria rivoluzione avendo introdotto procedure diverse sia per le modalità di accesso al P.C.T. sia per il nuovo sistema di comunicazione tra l'avvocato e il Gestore Centrale per lo scambio di informazioni e documenti.

4.1. Il passaggio dalla C.P.E.C.P.T. alla P.E.C.

Con la comunicazione resa nota da D.G.S.I.A. in data 17 ottobre 2011 veniva data di fatto attuazione, anche sotto il profilo sostanziale, alle nuove regole tecniche contenute nel D.M. n. 44/2011 indicandosi che, dal 19 novembre 2011,tutte le trasmissioni telematiche in ingresso ed in uscita (quindi sia depositi che comunicazioni) sarebbero avvenute unicamente attraverso il sistema della posta elettronica certificata e ciò nel rispetto delle specifiche tecniche emesse il 18 luglio 2011 da D.G.S.I.A.
Si specificava altresì che il "canale P.E.C." sarebbe stato attivato dal 7 novembre 2011 almeno per le sedi in cui erano attivi i servizi di trasmissione telematica.
Strano ma vero … la data indicata è stata rispettata!
Il modo migliore per spiegare in cosa consista tale passaggio è quello di porre a confronto i due sistemi di comunicazione.
Cominciamo col dire che C.P.E.C.P.T. altro non è che l'acronimo di **C**asella di **P**osta **E**lettronica **C**ertificata per il **P**rocesso **T**elematico così come P.E.C. lo è di **P**osta **E**lettronica **C**ertificata.
Fino a qui, a parte il nome, nessuna differenza tra **C.P.E.C.P.T. e P.E.C.** in quanto, l'una e l'altra **sono**, così come facilmente intuibile, **caselle di posta elettronica certificata**.
Vediamo allora di evidenziare le differenze non sul piano formale ma su quello sostanziale.

4.1.1. La C.P.E.C.P.T.

- era collocata all'interno del punto d'accesso al P.C.T. e accessibile solo ed esclusivamente tramite C.N.S. (Carta Nazionale dei Servizi) a seguito di controllo sulla identità del richiedente l'accesso tramite firma digitale;
- era consultabile in ambiente protetto all'interno del P.D.A. e quindi all'interno del Dominio Giustizia;

- veniva rilasciata dopo severi controlli sulla identità ed i requisiti del richiedente dal gestore del P.D.A. a seguito della richiesta di iscrizione del professionista al P.D.A. medesimo;
- il professionista non poteva incorrere in nessuna responsabilità quanto al suo funzionamento considerando che la stessa non poteva essere gestita dal titolare il quale ne disconosceva anche le credenziali non dovendo (potendo) quindi provvedere alla sua manutenzione;
- non poteva essere oggetto di SPAM, essendo di fatto segreta e accessibile, solo tramite P.D.A., all'interno del Dominio Giustizia;
- non poteva essere oggetto di virus normalmente contenuti negli allegati ai messaggi di posta elettronica.

4.1.2. La P.E.C.

- Viene rilasciata da un gestore privato;
- agisce all'esterno del P.D.A. e del Dominio Giustizia e può essere utilizzata per altri scopi ma, una volta noto l'indirizzo a terzi, potrà essere utilizzata da quest'ultimi anche per l'invio di messaggi che nulla abbiano a che fare con il P.C.T e quindi da ciò la concreta possibilità sia di ricevere spam sia virus tramite gli allegati ai messaggi di posta elettronica;
- la manutenzione ordinaria dovrà essere effettuata dal suo titolare il quale risponderà conseguentemente di eventuali malfunzionamenti;
- il titolare dovrà dotare tutti i terminali informatici, tramite i quali opererà con il P.C.T., di software idoneo a verificare l'assenza di virus per ogni messaggio in arrivo e in partenza e di software antispam idoneo a prevenire la trasmissione di messaggi di posta elettronica indesiderati;
- il titolare dovrà conservare **"con ogni mezzo idoneo"** le ricevute di avvenuta consegna dei messaggi trasmessi al dominio giustizia;
- il titolare dovrà dotarsi di servizio automatico di avviso dell'imminente saturazione della propria P.E.C. e, altresì, dovrà verificare l'effettiva disponibilità dello spazio disco a disposizione (almeno un giga).

All'esito del confronto è possibile affermare che:

1) la C.P.E.C.P.T. era senza dubbio più idonea, sicura e funzionale allo scambio di informazioni nel P.C.T avendo, di fatto, diminuito la sicurezza relativamente alle informazioni che vengono scambiate con il professionista nell'utilizzo del P.C.T.
2) con il passaggio dalla C.P.E.C.P.T. (casella di posta elettronica certificata del processo telematico) alla P.E.C. (posta elettronica certificata) come sistema di comunicazione nell'ambito del processo civile telematico (P.C.T.), definitivamente sancito dal D.M. 21 febbraio 2011, n. 44 e le successive regole tecniche pubblicate nel luglio 2011, si verifica anche il passaggio di importanti e pesanti responsabilità a carico del singolo professionista; a ciò si aggiunga che, con tale nuova forma di comunicazione il legislatore. Da ultimo evidenzio l'assoluta insufficienza e inadeguatezza dell'espressione **"con ogni mezzo idoneo"** contenuta nel n. 3 dell'art. 20, D.M. 21 febbraio 2011, n. 44 e più sopra richiamata essendo chiaro come tale disposizione nulla in realtà disponga sulle tecniche da adottare per la conservazione delle ricevute di avvenuta consegna dei messaggi trasmessi al dominio giustizia, lasciando quindi il professionista da solo e libero di scegliere le misure da adottare che, invece, il legislatore avrebbe dovuto indicare tassativamente sotto il profilo tecnico in considerazione dell'importanza dell'argomento oggetto della citata disposizione. Chi infatti potrà essere certo di aver ottemperato al precetto indicato dalla norma se la stessa nulla dice circa gli accorgimenti da adottare?

4.2. La natura e la funzione del P.D.A. prima e dopo il D.M. 21.02.2011 n. 44 - Il Portale dei Servizi Telematici

Il P.D.A., prima del D.M. 21 febbraio 2011 n. 44, altro non era che il punto di passaggio obbligatorio sotto forma di sito web attraverso il quale si doveva transitare (accedere) affinché fosse possibile utilizzare il processo telematico.
Poteva tecnicamente essere definito come la struttura tecnico-organizzativa che forniva ai soggetti abilitati esterni (avvocati, ausiliari del giudice, C.T.U., ecc.), secondo quanto previsto dalle regole tecnico operative emanate dal Ministro della Giustizia, l'accesso (mediante business key o smart card) ai servizi di consultazione e di trasmissione telematica degli atti previsti dal processo civile telematico.

4.2.1. Funzioni del P.D.A.

Tramite P.D.A. quindi:

- si garantiva l'autenticazione dei soggetti abilitati all'accesso;
- consentiva la consultazione dei registri di cancelleria (accesso al sistema Polisweb sincrono);
- consentiva il deposito degli atti telematici;
- consentiva la richiesta delle copie elettroniche e di quelle cartacee da ritirare presso le cancellerie;
- forniva la C.P.E.C.P.T. agli avvocati, esclusivamente dedicata alla ricezione delle comunicazioni telematiche da parte degli uffici giudiziari come previsto dal P.C.T.

In particolare il P.D.A. era in grado non solo di svolgere la fase della autenticazione dell'avvocato ma anche il ruolo (avvocato, praticante abilitato) nonché eventuali situazioni soggettive che impedissero all'avvocato di accedere al processo telematico (sospensione, revoca, cancellazione o radiazione o altro impedimento come tale riconosciuto dal locale Consiglio dell'Ordine).

4.2.2. Impossibilità, per professionisti e Ordini, di essere iscritti a più P.D.A. contemporaneamente

Ogni avvocato poteva quindi essere iscritto ad un solo P.D.A.; volendo cambiare avrebbe dovuto prima cancellare l'iscrizione al vecchio P.D.A. per poi richiedere l'iscrizione al nuovo.
Anche i Consigli degli Ordini potevano essere iscritti ad un solo P.D.A. in quanto:
dall'analisi del comma 1 dell'art. 17 del D.M. 17 luglio 2008[8] (comunicazioni dei Consigli dell'Ordine degli Avvocati e del C.N.F) si desumeva che "*Al fine dell'inserimento nei registri degli indirizzi elettronici, i consigli dell'ordine degli avvocati e il Consiglio nazionale forense comunicano al Ministero della giustizia ed ai punti di accesso di riferimento le informazioni e le loro variazioni, per via telematica, relative ai difensori*".
Il comma 5 dell'art. 17 del D.M. 17.07.08 prevedeva inoltre che "*La comunicazione di cui al comma 1 è inviata da una casella di posta elettronica certificata, UNIVOCA per ciascun consiglio dell'ordine degli avvocati, aderente alle specifiche tecniche riportate nell'allegato A, indicata con atto sottoscritto dal Presidente del Consiglio dell'Ordine*".
Successivamente al D.M. 17 luglio 2008 venivano rilasciate dal Ministero della Giustizia le SPECIFICHE PER L'INVIO DELL'ALBO AVVOCATI.

[8] http://www.giustizia.it/giustizia/it/mg_1_8_1.wp;jsessionid=34BD79444356C97C62038FA76CE17432.ajpAL01?facetNode_1=3_1_5&previsiousPage=mg_1_8&contentId=SDC84528.

Il punto 1.2 di tali specifiche (Accesso al Processo Civile Telematico: C.P.E.C.P.T. del C.D.O.) prevedeva che:
"*Per la funzionalità di invio dell'albo, ogni Consiglio dell'Ordine* […] *deve disporre di una Casella di Posta Elettronica Certificata del Processo Telematico (C.P.E.C.P.T.) per scambiare messaggi con il GC (Gestore Centrale)";* inoltre, "Il Rappresentante dell'Ordine o un suo delegato […] ha il compito di firmare l'albo in formato elettronico ed inviarlo al GC tramite la CPECPT predisposta per questa funzione". "L'accesso alla CPECPT è riservato al Rappresentante del CDO o ad un suo delegato, oppure ad un responsabile della struttura tecnica che gestisce il P.D.A. delegato dal CDO all'invio dell'albo. "Qualora il CDO non possegga un proprio P.D.A., può delegare un altro P.D.A. all'invio dell'albo… Il P.D.A. delegato all'invio dell'albo provvederà a creare la CPECPT e a darne comunicazione al CDO". "L'albo firmato dal Rappresentante del CDO (o da un suo delegato) sarà quindi trasmesso al GC tramite la CPECPT predisposta a tale funzione".
Dall'analisi di quanto sopra è palese che, quando un C.O.A. non possedeva un proprio P.D.A. delegava altro P.D.A. (esterno) all'invio dell'albo; il P.D.A. delegato doveva creare la CPEPCT attraverso la quale poi avrebbe inviato l'albo telematico al Ministero.
Ma, come sopra riportato, la CPECPT prevista dal comma 5 dell'art. 17 del D.M. 17.07.08 DOVEVA ESSERE UNIVOCA per ciascun Consiglio dell'Ordine.
Dall'univocità della CPEPCT si evince che un Consiglio dell'Ordine, non disponendo di un proprio P.D.A., potesse delegare solo un P.D.A. (e quindi essere iscritto ad un solo P.D.A.) in quanto se per l'Ordine fosse stato possibile delegare più P.D.A. l'invio dell'albo telematico, ogni P.D.A. si sarebbe dovuto munire di apposita CPECPT ma considerando che la CPECPT prevista dal comma 5 dell'art. 17 del D.M. 17.07.08 DOVEVA ESSERE UNIVOCA per ciascun Consiglio dell'Ordine, ciò non era possibile.

4.2.3. Il P.D.A. dopo il D.M. 21 febbraio 2011, n. 44

Con l'emanazione del D.M. 21 febbraio 2011 n. 44 - Pubblicato nella G.U. n. 89 del 18-04-2011 e delle successive specifiche tecniche riferite all'art. 34 del citato D.M. (provvedimento 18 luglio 2011 pubblicato per estratto sulla Gazzetta Ufficiale n. 175 del 29-7-2011 e in forma integrale sul sito internet istituzionale del Ministero della giustizia) per accedere al processo telematico la "chiave" non è più solo quella del P.D.A., ma anche il Portale dei Servizi Telematici del Ministero della Giustizia (D.M. art.6 D.M. 21.02.2011 n. 44).
L'avvocato viene riconosciuto dal portale dei Servizi Telematici attraverso identificazione informatica mediante carta d'identità elettronica o carta nazionale dei servizi (cfr. art. 6 delle specifiche tecniche del 18 luglio 2011 e art. 64 e segg. del codice dell'amministrazione digitale).
Viene meno, quindi, la funzione esclusiva e primaria del punto di accesso (P.D.A.) il quale ora dovrebbe offrire solo i servizi correlati al Consiglio dell'Ordine (come l'invio degli albi o le gestioni accentrate) ed agli avvocati come la "consolle" per predisporre ed inviare gli atti.

4.2.4. Il momento del passaggio dal vecchio al nuovo P.D.A. e dalla CPECPT alla PEC

La comunicazione inviata da D.G.S.I.A. il 17 ottobre 2011[9] segna inoltre il passaggio, dal 19 novembre 2011, dalla CPECPT alla PEC come mezzo di invio di tutte le trasmissioni telematiche (sia depositi che comunicazioni) e, di conseguenza anche il passaggio dal "vecchio" significato del P.D.A. al nuovo. Il professionista da tale data non sarà più obbligato ad accedere al processo

[9] http://www.processotelematico.giustizia.it/pdapublic/index.jsp?sid=3&nid=157&y=2011&m=9&d=21

telematico attraverso il tradizionale P.D.A. esterno ma potrà farlo, come sopra anticipato, utilizzando il Portale dei Servizi Telematici del Ministero della Giustizia (art. 6 del D.M. 21 febbraio 2011 n. 44 e art. 5 delle specifiche tecniche del 18 luglio 2011) considerando che il P.D.A. non dovrà più rilasciare la CPECPT che prima del 19 novembre 2011 era l'unico mezzo utilizzato con valore legale per le trasmissioni telematiche.

4.2.5. Il Portale dei Servizi Telematici e l'utilità del P.D.A. dopo il D.M. 21.02.2011 n. 44

Dalla comunicazione e dalle normative richiamate sembrerebbe non più utile o necessario per il professionista o un Consiglio dell'Ordine essere iscritto ad un P.D.A. e ciò in considerazione del fatto che il Ministero della Giustizia ha realizzato, per accedere al PCT, il Portale dei Servizi Telematici.
Ma, attenzione in quanto il portale dei servizi telematici può solo:

- consentire l'accesso da parte dell'utente privato alle informazioni e ai provvedimenti giudiziari (art. 6, n. 1, D.M. 21 febbraio 2011, n. 44);
- mettere a disposizione dei soggetti abilitati esterni i servizi di consultazione, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34 (art. 6, n. 3, D.M. 21 febbraio 2011, n. 44);
- mettere a disposizione i servizi di pagamento telematico (art. 6, n. 4, D.M. 21 febbraio 2011, n. 44);
- mettere a disposizione i documenti che contengono dati sensibili oppure che eccedono le dimensioni del messaggio di posta elettronica certificata (art. 6, n. 5, D.M. 21 febbraio 2011, n. 44);
- consentire l'accesso senza l'impiego di apposite credenziali, sistemi di identificazione e requisiti di legittimazione, alle informazioni ed alla documentazione sui servizi telematici del dominio giustizia, alle raccolte giurisprudenziali e alle informazioni essenziali sullo stato dei procedimenti pendenti, che vengono rese disponibili in forma anonima (art. 6, n. 6, D.M. 21 febbraio 2011 n. 44).

Come si vede nessun riferimento viene fatto circa l'esistenza, all'interno del Portale dei Servizi Telematici, di utilità o software attraverso cui sia possibile redigere l'atto telematicamente e preparare la busta telematica operazioni queste necessarie e senza le quali non sarebbe possibile spedire telematicamente atti o documenti al Gestore dei Servizi Telematici e, da questo, al Gestore locale (Ufficio Giudiziario competente a ricevere l'atto o il documento).
A ciò deve aggiungersi che il passaggio dalla CPECPT alla PEC, come mezzo trasmissione telematico sia per i depositi che per le comunicazioni, ha sicuramente complicato le cose per gli addetti ai lavori in quanto soprattutto (ma non solo) la gestione delle quattro ricevute che si ottengono per ogni deposito telematico effettuato risultare difficile, anche a causa della necessità per il singolo avvocato di dover provvedere da solo alla corretta configurazione di tutti i programmi di posta elettronica installati sui vari dispositivi in uso, al fine di non perdere il controllo dei dati e, soprattutto le ricevute elettroniche costituendo queste ultime l'unico mezzo di prova idoneo a dimostrare l'avvenuto deposito di un determinato atto o documento.
E' possibile affermare che tale Portale ad oggi sia idoneo solo per la CONSULTAZIONE di atti e/o documenti ma non anche a quella preparatoria, propedeutica e successiva al deposito degli stessi.
La logica conseguenza è che i P.D.A. esterni continueranno a svolgere (come fino ad ora hanno svolto) una funzione importantissima soprattutto se consentiranno al professionista di utilizzare, con maggiore facilità, tutte le attività legate all'utilizzo del processo telematico tramite consolle che consenta, ad esempio, di poter disporre di sistemi attraverso cui:

- acquisire automaticamente da Polisweb le udienze e le scadenze relative, permettendo inoltre di annotare autonomamente gli appuntamenti, le udienze, le attività e le scadenze, collegandole anche al fascicolo a cui si riferiscono;
- permettere agli avvocati di utilizzare la propria casella di posta elettronica certificata arricchita di funzioni specifiche per il Processo Civile Telematico in grado di semplificare la comunicazione con il gestore PEC del Ministero rendendo possibile, ad esempio, effettuare un deposito di un atto attraverso una semplice procedura che provvederà ad archiviare in modo razionale le varie e-mail di risposta (ricevute).
- Operare senza l'utilizzo di software residenti sul proprio PC ma con web application che consentano al professionista l'utilizzo delle funzioni del PCT a prescindere dal fatto che disponga o meno del proprio computer o che si trovi o meno nel suo studio.

4.2.5. Nuove regole tecniche e adempimenti del C.O.A.

Con l'introduzione delle nuove regole e specifiche tecniche, più volte citate, anche gli Ordini degli Avvocati (ma non solo) hanno dovuto eseguire determinati per consentire al professionista la consultazione del Polisweb e operare con il processo telematico.
A tal proposito il Ministero della Giustizia diramava il giorno 21 ottobre 2011, mediante pubblicazione sul sito dedicato al processo telematico, avviso con il quale ***"Si informa che l'invio degli albi e degli elenchi contenenti l'indirizzo di posta elettronica certificata, che alimenta il Registro Generale degli Indirizzi elettronici, ai sensi dell'art. 8 comma 3 del provvedimento 18 luglio 2011 ("specifiche tecniche"), è possibile a partire dal giorno 25 ottobre 2011 e comunque soltanto dopo aver effettuato il censimento di cui ai commi 1 e 2 dello stesso articolo e aver quindi ricevuto la risposta di cui al comma 3"*.**
L'Ordine ha dovuto quindi effettuare il censimento previsto dall'art. 8 comma 3 delle specifiche tecniche del 18 luglio 2011 utilizzando il modulo di censimento messo a disposizione per il download dal Ministero.
Il modello da compilare prevedeva (e prevede) i seguenti campi:

1. Dati identificativi

a) Codice Ente : Il codice ente è formato dal prefisso "C.O.A." al quale va aggiunto il codice ISTAT del comune di riferimento per il CdO. La lista dei codici è consultabile dal sito web dell'Istituto Nazionale di Statistica www.istat.it.
b) Descrizione : Il campo Descrizione è precompilato, si dovrà aggiungere soltanto il comune di riferimento per il CdO.
c) Codice fiscale : è il codice fiscale del Consiglio dell'Ordine

2. Dati del delegato alla firma ed all'invio dell'albo

Il CdO delega ad un rappresentante le funzioni di firma digitale e di inoltro dell'albo e dei suoi aggiornamenti. Il delegato dovrà quindi essere in possesso di un dispositivo di firma digitale valido e avere accesso alla casella di posta elettronica certificata che verrà utilizzata per l'inoltro dell'albo e dei suoi aggiornamenti.

a) Nominativo: completare il campo inserendo nome e cognome del delegato alla firma ed all'invio dell'albo e dei suoi aggiornamenti
b) Codice fiscale: inserire il codice fiscale del delegato

È possibile delegare più soggetti alla firma/invio dell'albo, basterà duplicare i campi previsti per il censimento e compilarli indicando i dati degli altri soggetti da censire.

3. Dati relativi all'invio

a) Indirizzo della casella di posta elettronica certificata : Indicare l'indirizzo della casella di posta certificata che il delegato all'invio utilizzerà per l'inoltro dell'albo e dei suoi aggiornamenti. A tale scopo è consigliabile utilizzare una casella certificata a disposizione del CdO o crearne una nuova che verrà dedicata all'inoltro degli albi.
Il documento di censimento deve essere sottoscritto dal Presidente del CdO ed inviato unicamente per via telematica all'indirizzo di posta certificata che la D.G.S.I.A. rende disponibile a tale scopo.
Il Presidente del CdO dovrà sottoscrivere il documento con firma autografa, quindi scannerizzare il modello in formato pdf ed eseguire l'inoltro per via telematica al seguente indirizzo di posta certificata: prot.dgsia.dog@giustiziacert.it.
Terminate le operazioni di censimento l'Ordine riceve una risposta dalla D.G.S.I.A., in caso di esito positivo si dovrà procedere all'invio dell'albo e dei relativi indirizzi di posta certificata degli iscritti, in formato xml e nel rispetto della normativa che disciplina le nuove regole tecniche per il Processo Civile Telematico- La struttura, il contenuto ed il formato del file (*ComunicazioniSoggetti.xlm)* contenente l'elenco degli iscritti e dei relativi indirizzi di posta certificata sono regolati dal provvedimento del 18 luglio 2011, art. 7 e 8.
L'indirizzo al quale inviare il file così predisposto (tramite la casella di posta elettronica certificata indicata nel documento di censimento) è comunicazionesoggetti@civile.ptel.giustiziacert.it.
Allo stesso modo e sempre seguendo la struttura ed il formato previsti dalle regole tecniche, andranno predisposti ed inoltrati gli aggiornamenti periodici delle anagrafiche e dei relativi indirizzi di posta certificata.
Il file dovrà contenere i seguenti campi:

- codice fiscale
- operazione (può valere: - A (inserimento) - C (cancellazione) - M (modifica). Nel caso di invio dell'intero albo il campo è ignorato e tutti i record sono considerati come da inserire. Il campo è preso in considerazione SOLO in caso di invio albo integrativo).
- cognome
- nome
- stato avvocato (A=attivo;S=sospeso;R=radiato)
- Casella PEC
- Ruolo
- indirizzo residenza
- CAP residenza
- comune residenza
- provincia residenza
- data di nascita
- comune di nascita
- provincia di nascita
- indirizzo domicilio legale 1
- CAP domicilio legale 1
- comune domicilio legale 1
- provincia domicilio legale 1

E' importante che tutti i campi sopra riportati siano privi di anomalie in quanto il Ministero prevede una validazione (controllo) non per singolo dato di avvocato inserito ma sull'intero file XML.
Ciò significa che anche un solo nominativo con dati non conformi alle specifiche ministeriali avrà come conseguenza il rifiuto dell'intero albo.

A ogni invio corrisponde una risposta tramite PEC; il messaggio ha come oggetto la medesima descrizione del messaggio originale con il suffisso "– Esito" e riporta in allegato l'esito della elaborazione del messaggio con le eventuali eccezioni;
L'esito si riferisce sia ad errori presenti sui dati, quindi riconducibili alle informazioni dei singoli soggetti (come ad esempio codice fiscale inesistente), sia ad errori legati a vincoli e prerequisiti che presuppongono la validità dell'invio di un albo (ad esempio: censimento dell'ente richiedente e dei soggetti abilitati all'invio dell'albo).
Ad ogni nuovo indirizzo di PEC registrato nelle anagrafiche a seguito dell'inserimento di un nuovo soggetto o di modifica di uno esistente, viene inviato un messaggio di cortesia.
D.G.S.I.A., in caso di errore, invierà il seguente messaggio:
il file Comunicazioni Soggetti non è conforme allo schema XSD
CODICE ERRORE: F003
DESCRIZIONE: Errore file non conforme allo schema.
La cosa più grave è che non verrà indicato quali siano i nominativi con i dati non conformi e, conseguentemente, neanche quali siano i dati non conformi.
Ad oggi pare che incontrino il rifiuto dell'albo per mancanza di conformità alle specifiche ministeriali i record che abbiano:

- il campo provincia vuoto o che presenti caratteri numerici;
- indirizzo di studio o residenza privi di indicazione della via;
- i numeri telefoni con il prefisso + .

Solo l'invio (validato in ricezione dal Ministero) dell'albo digitale consentirà agli iscritti dell'Or-dine di poter accedere, dal 19 novembre 2011, al POLISWEB e poter usufruire del PCT; è auspicabile che, per alcuni giorni seguenti al 19 novembre 2011 il Ministero, pur in mancanza della ricezione del detto albo digitale, consenta almeno la consultazione del Polisweb.

4.2.6. Processo Telematico e Cloud Computing

A questo proposito saranno sicuramente da prediligere i P.D.A. che consentiranno l'accesso e l'utilizzo dei servizi online e non tramite software installati e residenti sul pc; così facendo l'avvocato avrà la possibilità di accedere e interagire con il processo telematico da qualsiasi pc e da qualsiasi parte del mondo avendo cura, naturalmente, di avere con se la "chiave di accesso" (firma digitale); in questo modo non sarà necessario installare in tutti i pc dello studio i software tramite i quale accedere al processo telematico cosa questa che,

1) consentirà di economizzare i costi considerando che, come avviene per altri software, ad ogni ulteriore installazione su diverso pc corrisponde un costo ulteriore da sostenere e,
2) in caso di problemi o malfunzionamenti del pc ove il software è installato, eviterà di rimanere inoperativi potendo utilizzare un qualsiasi altro computer, finanche quello dei c.d. internet caffè.
   Non dobbiamo dimenticare che ormai sempre più si parla di CLOUD COMPUTING, ossia l'insieme di tecnologie che permettono, tipicamente sotto forma di un servizio offerto al cliente, di memorizzare/archiviare e/o elaborare dati grazie all'utilizzo di risorse distribuite e accessibili in rete.

Capitolo V
Il sistema cloud computing

Sommario: 1. Premessa - 2. Che cosa è il cloud computing - 3. Esternalizzare i dati nelle cloud pubbliche – 4. I diversi modelli di servizio – 5. Innovare governando i rischi – 6. Indicazioni per l'utilizzo consapevole dei servizi

Alla fine del precedente capitolo ho, genericamente, descritto l'importanza di poter utilizzare in cloud computing gli strumenti necessari per interagire con il processo telematico.
A tal proposito credo sia utile far conoscere al lettore, riportandolo integralmente, il documento del giugno 2011 elaborato dal Garante per la Protezione dei Dati Personali che spiega come utilizzare consapevolmente i servizi offerti in cloud computing.

Garante per la protezione dei dati personali
"Cloud computing: indicazioni per l'utilizzo consapevoli dei servizi"[10]

1. Premessa
L'Autorità nell'ottica di promuovere un utilizzo corretto delle nuove modalità di erogazione dei servizi informatici, specie per quelli erogati tramite cloud pubbliche (public cloud), che comportano l'esternalizzazione di dati e documenti, ritiene opportuna e doverosa un'opera di informazione orientata a tutelare l'importante patrimonio informativo costituito dai dati personali.
Tali indicazioni si propongono, quindi, di offrire un primo insieme di indicazioni utili a tutti gli utenti di dimensioni contenute e di limitate risorse economiche (singoli, piccole o medie imprese, amministrazioni locali quali i piccoli comuni, ecc.) destinatari della crescente offerta di servizi di cloud computing (pubbliche o ibride), con l'obiettivo di favorire l'adozione consapevole e responsabile di tale tipologia di servizi.
Le avvertenze di seguito enucleate costituiscono un primo quadro di cautele che favoriscono il corretto trattamento dei dati personali attraverso l'utilizzo dei predetti servizi virtuali e, pertanto, si indirizzano anche ai fornitori, i quali possono fare riferimento a tali indicazioni nella predisposizione dei loro servizi, con l'accortezza di informare opportunamente gli utenti in ordine alla loro adozione.
L'Autorità - nella consapevolezza che l'utilizzo dei servizi di cloud computing prefigura problematiche ben difficilmente risolvibili a livello nazionale che richiedono, invece, una riflessione condivisa a livello sia europeo sia internazionale, e in considerazione di tutte le sue implicazioni in relazione al trattamento dei dati personali – intende in ogni caso continuare a seguire l'evoluzione del fenomeno, anche partecipando con altri decisori istituzionali a specifici tavoli di lavoro aperti in materia, in particolare con DigitPA per quanto attiene all'adozione di modelli orientati alle cloud in ambito pubblico. L'Autorità, inoltre, si riserva, laddove ne rilevasse la necessità, di adottare in futuro specifiche e dettagliate prescrizioni indirizzate a utenti e fornitori, specie sotto il profilo delle misure di sicurezza.

[10] http://www.garanteprivacy.it/garante/document?ID=1819933

2. Che cosa è il cloud computing?

L'evoluzione delle tecnologie informatiche e dei mezzi di comunicazione è inarrestabile e ogni giorno vengono messi a disposizione dei cittadini nuovi strumenti e soluzioni sempre più sofisticate e integrate con la rete Internet, che consentono di soddisfare crescenti esigenze di informatizzazione e di comunicazione.

In tale quadro, il cloud computing è un insieme di modelli di servizio che più di altri si sta diffondendo con grande rapidità tra imprese, pubbliche amministrazioni e cittadini perché incoraggia un utilizzo flessibile delle proprie risorse (infrastrutture e applicazioni) o di quelle messe a disposizione da un fornitore di servizi specializzato.

L'innovazione e il successo delle cloud (le nuvole informatiche) risiede nel fatto che, grazie alla raggiunta maturità delle tecnologie che ne costituiscono la base, tali risorse sono facilmente configurabili e accessibili via rete, e sono caratterizzate da particolare agilità di fruizione che, da una parte semplifica significativamente il dimensionamento iniziale dei sistemi e delle applicazioni mentre, dall'altra, permette di sostenere gradualmente lo sforzo di investimento richiesto per gli opportuni adeguamenti tecno-logici e l'erogazione di nuovi servizi.

Nell'ambito del cloud computing è ormai prassi consolidata distinguere tra private cloud e public cloud.

Una private cloud (o nuvola privata) è un'infrastruttura informatica per lo più dedicata alle esigenze di una singola organizzazione, ubicata nei suoi locali o affidata in gestione ad un terzo (nella tradizionale forma dell'hosting dei server) nei confronti del quale il titolare dei dati può spesso esercitare un controllo puntuale. Le *private cloud* possono essere paragonate ai tradizionali "data center" nei quali, però, sono usati degli accorgimenti tecnologici che permettono di ottimizzare l'utilizzo delle risorse disponibili e di potenziarle attraverso investimenti contenuti e attuati progressivamente nel tempo.

Nel caso delle public cloud, invece, l'infrastruttura è di proprietà di un fornitore specializzato nell'erogazione di servizi che mette a disposizione di utenti, aziende o amministrazioni - e quindi condivide tra di essi - i propri sistemi attraverso l'erogazione via web di applicazioni informatiche, di capacità elaborativa e di stoccaggio. La fruizione di tali servizi avviene tramite la rete Internet e implica il trasferimento dell'elaborazione o dei soli dati presso i sistemi del fornitore del servizio, il quale assume un ruolo importate in ordine all'efficacia delle misure adottate per garantire la protezione dei dati che gli sono stati affidati. In questo caso l'utente insieme ai dati, infatti, cede una parte importante del controllo esercitabile su di essi. Ad esempio, la complessità delle infrastrutture, e la loro eventuale dislocazione su siti al di fuori dei confini nazionali potrebbe determinare l'impossibilità sia di conoscere con esattezza l'ubicazione dei propri dati nella nuvola, sia di sapere se e quando i dati vengono spostati da un luogo all'altro per esigenze organizzative, tecniche o economiche difficilmente determinabili e gestibili a priori. Inoltre, la dimensione del fornitore potrebbe condizionare la forza contrattuale dei fruitori del servizio e la loro possibilità di esercitare un controllo diretto, seppur concordato, sui siti e sulle infrastrutture utilizzate per ospitarne i dati.

Acquisire servizi cloud significa acquistare presso un fornitore di servizio risorse (ad esempio server virtuali o spazio disco) oppure applicazioni (ad esempio posta elettronica e strumenti per l'ufficio).

- I dati non risiedono più su server "fisici" dell'utente, ma sono allocati sui sistemi del fornitore (a meno di copie in locale)
- L'infrastruttura del fornitore del servizio è condivisa tra molti utenti per cui sono fondamentali adeguati livelli di sicurezza
- L'utilizzo del servizio avviene via web tramite la rete Internet che assume dunque un ruolo centrale in merito alla qualità dei servizi fruiti ed erogati

- I servizi acquisibili presso il fornitore del servizio sono a consumo e in genere è facile far fronte ad eventuali esigenze aggiuntive (ad esempio più spazio disco o più potenza elaborativa)
- Esternalizzare i dati in remoto non equivale ad averli sui propri sistemi: oltre ai vantaggi, ci sono delle controindicazioni che bisogna conoscere.

Accanto alle private e public cloud si annoverano nuvole "intermedie" quali le cloud ibride (o hybrid cloud), caratterizzate da soluzioni che prevedono l'utilizzo di servizi erogati da infrastrutture private accanto a servizi acquisiti da cloud pubbliche, e le community cloud in cui l'infrastruttura è condivisa da diverse organizzazioni a beneficio di una specifica comunità di utenti.
I potenziali vantaggi del cloud computing certamente possono promuovere la sistematizzazione delle infrastrutture, la riorganizzazione dei flussi informativi, la razionalizzazione dei costi e quindi in generale favorire nel caso sia del mondo imprenditoriale, sia della pubblica amministrazione servizi più moderni, efficienti e funzionali in linea con le esigenze di crescita di un moderno Sistema Paese.
È d'altra parte assodato che il cloud computing non è un fenomeno temporaneo o una moda, ma il passo successivo dell'evoluzione nel modo in cui si utilizza la Rete Internet, che da strumento per la sola condivisione documentale (la pagina web resa disponibile dal sito web remoto) diviene la porta d'accesso alle risorse elaborative di un provider di servizi (l'applicazione resa disponibile in modalità web).
Questa trasformazione sta determinando una "modifica dei costumi" che è già in atto ed è più evidente nell'utenza individuale che più frequentemente, ma non sempre con completa consapevolezza anche dei possibili rischi derivanti dalle nuove tecnologie utilizzate, si avvale di servizi erogati da fornitori terzi (public cloud) per far fronte alle sue esigenze informative: l'utente consumer, infatti, utilizza i social network sui quali trasferisce abitualmente foto, informazioni, idee e opinioni, usa strumenti di elaborazione documentale via web, impiega gli hard-disk remoti per poter sempre disporre dei propri documenti da qualunque dispositivo e in qualunque luogo si trovi, si avvale delle applicazioni per i moderni smartphone sempre connessi ad Internet che tramite l'associazione delle informazioni di geolocalizzazione all'utente hanno aperto la strada a innovative funzionalità, anche in ambito sociale.
Risulta d'altra parte evidente come l'offerta degli operatori economici stia incalzando il mercato delle imprese e della Pubblica Amministrazione con soluzioni che incoraggiano l'acquisizione di servizi esternalizzati, utilizzando come volano verso i nuovi investimenti la prospettiva di risparmi legati alla sostituzione o all'affianca-mento degli asset per il trattamento delle informazioni tradizionalmente nel diretto possesso dell'utente, con soluzioni acquisite a consumo presso terzi.
È tuttavia opportuno evidenziare come il ricorso a quelle modalità che intrinsecamente promuovono l'utilizzo di servizi esternalizzati comportino anche la migrazione dei dati dai sistemi locali sotto il diretto controllo dell'utente, impresa o amministrazione ai sistemi remoti del provider di servizi.

3. Esternalizzare i dati nelle cloud pubbliche

Come sopra delineato, le public cloud (o nuvole informatiche pubbliche) sono infrastrutture controllate da organizzazioni che le rendono disponibili a terzi attraverso la vendita di servizi a consumo. Lo spazio virtuale e la capacità di elaborazione della "nuvola" sono condivisi tra molti utenti, singoli o appartenenti a imprese o enti diversi che accedono a tali risorse dell'infrastruttura tramite l'utilizzo della rete Internet.
Più precisamente, con il termine cloud computing o semplicemente cloud nell'ambito di questo documento ci si riferisce a un insieme di tecnologie e di modelli di servizio che:

- favoriscono la fruizione e l'erogazione di applicazioni informatiche, di capacità elaborativa e di stoccaggio via web;
- promuovono a seconda dei casi il trasferimento dell'elaborazione o della sola conservazione dei dati dai computer degli utenti ai sistemi del fornitore dei servizi.

La flessibilità e la semplicità con cui è possibile configurare i sistemi in cloud ne rende possibile un dimensionamento "elastico", attuato cioè secondo logiche di adattabilità alle contestuali esigenze e di fruizione a consumo. Gli utenti non devono curarsi della gestione dei sistemi informatici che, essendo utilizzati secondo la logica dell'esternalizzazione (outsourcing), sono completamente gestiti dai soggetti terzi nella cui nuvola sono conservati i dati. Generalmente, nel caso frequente di fornitori di grosse dimensioni dotati di infrastrutture complesse, la nuvola può estendersi geograficamente su siti distinti e l'utente potrebbe ignorare dove vengono effettivamente conservati i propri dati.
I servizi offerti dai fornitori di soluzioni di cloud computing sono molto diversificati, in costante e significativo aumento e spaziano da sistemi elaborativi virtuali, che sostituiscono o si affiancano ai tradizionali elaboratori ubicati nei locali propri dell'organizzazione, a servizi di supporto allo sviluppo e per l'hosting evoluto delle applicazioni, sino a soluzioni software rese disponibili in modalità web che sono sostitutive delle tradizionali applicazioni installate sui computer di utenti, imprese e di amministrazioni, quali ad esempio applicazioni per l'elaborazione dei testi, per la gestione di agende e calendari, eventualmente condivisi, cartelle per l'archiviazione dei documenti on-line, e persino soluzioni esternalizzate di posta elettronica. I dati trasferiti e archiviati per mezzo di questi servizi web presso il service provider possono essere trattati dagli utenti in remoto attraverso la rete Internet spesso senza la necessità di installare specifici programmi sui propri sistemi e senza l'esigenza di dover effettuare gli aggiornamenti software e tutte le altre attività correlate alla manutenzione e alla gestione delle infrastrutture informatiche.

4. I diversi modelli di servizio

Sul mercato, a seconda delle esigenze dell'utente, sono disponibili varie soluzioni di cloud computing erogate secondo modalità che ricadono in linea di massima in tre categorie, dette "modelli di servizio". Comunemente tali modelli di servizio sono riferiti sia a soluzioni di private cloud che di public cloud, ma vengono qui illustrati in un'ottica maggiormente aderente a quest'ultima tipologia di servizi, che prevede l'utilizzo condiviso da parte di utenti, imprese e soggetti pubblici dei sistemi di provider di servizi terzi.

- Nel caso di servizi IaaS (Cloud Infrastructure as a Service – infrastruttura cloud resa disponibile come servizio), il fornitore noleggia un'infrastruttura tecnologica, cioè server virtuali remoti che l'utente finale può utilizzare con tecniche e modalità che ne rendono semplice, efficace e produttiva la sostituzione o l'affiancamento ai sistemi già presenti nei locali dell'azienda. Tali fornitori sono in genere operatori di mercato specializzati che realmente dispongono di un'infrastruttura fisica, complessa e spesso distribuita in aree geografiche diverse.
- Negli SaaS (Cloud Software as a Service - software erogato come servizio della cloud), il fornitore eroga via web una serie di servizi applicativi ponendoli a disposizione degli utenti finali. Tali servizi sono spesso offerti in sostituzione delle tradizionali applicazioni installate localmente dall'utente sui propri sistemi, che è quindi spinto ad "esternalizzare" i suoi dati affidandoli al fornitore. Si pensi, ad esempio, ad applicazioni tipiche per l'ufficio erogate in modalità web quali fogli di calcolo, elaborazione dei testi, applicazioni per il protocollo informatico, la rubrica dei contatti e i calendari condivisi, ma anche alle moderne offerte di posta elettronica cloud.

- Infine, nei PaaS (Cloud platform as a service - piattaforme software fornite via web come servizio), il fornitore offre soluzioni per lo sviluppo e l'hosting evoluto di applicazioni. In genere questo tipo di servizi è rivolto a operatori di mercato che li utilizzano per sviluppare e ospitare soluzioni applicative proprie, allo scopo di assolvere a esigenze interne oppure per fornire a loro volta servizi a terzi. Anche nel caso dei PaaS il servizio erogato dal fornitore elimina la necessità per il fruitore di doversi dotare internamente di strumenti hardware o software specifici o aggiuntivi.

5. Innovare, governando i rischi

L'utilizzo di servizi di cloud computing è un fenomeno in forte ascesa e determina un cambio di mentalità nelle modalità di utilizzo della rete Internet che, da strumento di condivisione documentale, diviene la porta di accesso alle risorse elaborative e di stoccaggio di fornitori di servizi remoti.

Tale tipologia di servizi comporta la migrazione di dati dai sistemi locali sotto il diretto controllo dell'utente ai sistemi remoti del fornitore, che assume un ruolo centrale in ordine alla sicurezza dei dati e, quindi, all'adozione delle misure necessarie a garantirla. Tuttavia, è bene evidenziare come l'adozione di servizi esternalizzati non esime le imprese e le amministrazioni pubbliche che se ne avvalgono per la gestione del proprio patrimonio informativo dalle responsabilità che vengono loro attribuite, in particolare, dalla disciplina in materia di protezione dei dati personali.

I trattamenti di dati personali richiedono, infatti, sempre un'attenta ponderazione dei rischi legati alla sicurezza e alla fruibilità delle informazioni, indipendentemente dalle modalità di trattamento. Pertanto, vanno tenute in debito conto le particolari caratteristiche delle nuove tecnologie, allo scopo di governare i potenziali pericoli che possono derivare da utilizzi scarsamente consapevoli e da modelli innovativi adottati con metodi, prassi e processi non ancora sufficientemente consolidati e in grado di mitigare le eventuali criticità. È quindi opportuno, anche nel caso del cloud computing, razionalizzarne le peculiarità al fine di individuare i potenziali rischi insiti in tali servizi e quindi poter adottare efficaci e specifiche misure di prevenzione.

Nel caso del cloud computing, il trasferimento dei dati dai computer locali, nella fisica disponibilità e nel diretto controllo esercitabile dal titolare, verso sistemi remoti di proprietà di un terzo fornitore del servizio, presenta, accanto a potenziali utilità, anche i seguenti aspetti che necessitano di specifica attenzione:

- l'utente, affidando i dati ai sistemi di un fornitore remoto, ne perde il controllo diretto ed esclusivo; la riservatezza e la disponibilità delle informazioni allocate sulla nuvola certamente dipendono anche dai meccanismi di sicurezza adottati dal service provider ;
- il servizio prescelto potrebbe essere il risultato finale di una catena di trasformazione di servizi acquisiti presso altri service provider, diversi dal fornitore con cui l'utente stipula il contratto di servizio; l'utente a fronte di filiere di responsabilità complesse potrebbe non sempre essere messo in grado di sapere chi, dei vari gestori dei servizi intermedi, può accedere a determinati dati;
- il servizio virtuale, in assenza di adeguate garanzie in merito alla qualità della connettività di rete, potrebbe occasionalmente risultare degradato in presenza di elevati picchi di traffico o addirittura indisponibile laddove si verifichino eventi anomali quali, ad esempio, guasti, impedendo l'accessibilità temporanea ai dati in esso conservati;
- le cloud sono sistemi e infrastrutture condivise basate sul concetto di risorse noleggiate a un'utenza multipla e mutevole; i fornitori, infatti, custodiscono dati di singoli e di organizzazioni diverse che potrebbero avere interessi ed esigenze differenti o persino obiettivi contrastanti e in concorrenza;

- la conservazione dei dati in luoghi geografici differenti ha riflessi immediati sia sulla normativa applicabile in caso di contenzioso tra l'utente e il fornitore, sia in relazione alle disposizioni nazionali che disciplinano il trattamento, l'archiviazione e la sicurezza dei dati;
- l'adozione da parte del fornitore del servizio di tecnologie proprie può, in taluni casi, rendere complessa per l'utente la transizione di dati e documenti da un sistema cloud ad un altro o lo scambio di informazioni con soggetti che utilizzino servizi cloud di fornitori differenti, ponendone quindi a rischio la portabilità o l'interoperabilità dei dati.

Il fornitore, in base alla tipologia dei servizi offerti, assume la responsabilità di preservare la riservatezza, l'integrità o la disponibilità dei dati; pertanto, l'utente al momento della stipula dei contratti di servizio dovrà tenere in debito conto gli accorgimenti previsti per garantire il corretto trattamento dei dati immessi nella cloud.
Prima di adottare un sistema basato nel cloud computing è necessario, quindi, valutare attentamente il rapporto tra rischi e benefici derivante dall'utilizzo del predetto servizio virtuale, minimizzando i primi attraverso una attenta verifica dell'affidabilità del fornitore di servizi al quale ci si intende affidare.

6. Indicazioni per l'utilizzo consapevole dei servizi cloud

- **Ponderare prioritariamente rischi e benefici dei servizi offerti**

Prima di optare per l'adozione di servizi di cloud computing, è opportuno che l'utente verifichi la quantità e la tipologia di dati che intende esternalizzare (es. dati personali identificativi o meno, dati sensibili oppure particolarmente delicati come quelli genetici o biometrici, dati critici per la propria attività come ad esempio progetti riservati). E' necessario innanzitutto valutare gli eventuali rischi e le possibili conseguenze derivanti da tale scelta sotto il profilo della riservatezza e della loro rilevanza nel normale svolgimento della propria attività. Tale analisi valutativa dovrà evidenziare l'opportunità o meno di ricorrere a servizi cloud (limitandone l'uso ad esempio a determinati tipi di dati), nonché l'impatto sull'utente in termini economici e organizzativi, l'indisponibilità, pur se parziale o per periodi limitati, dei dati esternalizzati o, peggio, la loro perdita o cancellazione.

- **Effettuare una verifica in ordine all'affidabilità del fornitore**

Gli utenti dovrebbero ragionevolmente accertare l'affidabilità del fornitore prima di migrare sui sistemi virtuali i propri dati più importanti, tenendo in considerazione le proprie esigenze istituzionali o imprenditoriali, la quantità e la tipologia delle informazioni che intendono allocare nella cloud, i rischi e le misure di sicurezza. In funzione della tipologia di servizio che necessitano, oltre che della criticità dei dati, è opportuno che valutino la stabilità societaria del fornitore, le referenze, le garanzie offerte in ordine alla confidenzialità dei dati e alle misure adottate per garantire la continuità operativa a fronte di eventuali e imprevisti malfunzionamenti.
Gli utenti dovrebbero valutare, inoltre, le caratteristiche qualitative dei servizi di connettività di cui si avvale il fornitore in termini di capacità e affidabilità. Ulteriori criteri in base ai quali è possibile valutare l'affidabilità di un fornitore emergono dall'impiego di personale qualificato, dall'adeguatezza delle infrastrutture informatiche e di comunicazione, dalla disponibilità ad assumersi responsabilità, esplicitamente previste dal contratto di servizio, derivanti da eventuali falle nel sistema di sicurezza o a seguito di interruzioni di servizio.

- **Privilegiare i servizi che favoriscono la portabilità dei dati**

E' consigliabile ricorrere a servizi di cloud computing nelle modalità SaaS, PaaS o IaaS in un'ottica lungimirante, vale a dire privilegiando servizi basati su formati e standard aperti, che facilitino la

transizione da un sistema cloud ad un altro, anche se gestiti da fornitori diversi. Ciò al fine di scongiurare il rischio che eventuali modifiche unilaterali dei contratti di servizio da parte di uno qualunque degli operatori che intervengono nella catena di fornitura si traducano in condizioni peggiorative vincolanti o, comunque, per facilitare eventuali successivi passaggi da un fornitore all'altro.

- **Assicurarsi la disponibilità dei dati in caso di necessità**

Nell'utilizzo dei servizi di cloud computing, in assenza di stringenti vincoli sulla qualità formalizzati attraverso il contratto con il fornitore, si raccomanda di mantenere una copia di quei dati (anche se non personali) dalla cui perdita o indisponibilità potrebbero conseguire danni economici, per l'immagine o in generale relativi alla missione e alle finalità perseguite dall'utente. Ciò specie quando ci si affidi a servizi gratuiti o a basso costo quali, ad esempio, a servizi di hard-disk remoto, mail, soluzione per la conservazione documentale e così via, che potrebbero non presentare adeguate garanzie di disponibilità e prestazioni tipiche, invece, dei servizi professionali. Certamente, nel caso in cui i dati trattati non siano i propri, come avviene per aziende e pubbliche amministrazioni che raccolgono e detengono informazioni di terzi, l'adozione di servizi che non offrono adeguate garanzie di riservatezza e di continuità operativa può avere rilevanti ripercussioni nel patrimonio informativo dei soggetti cui i dati si riferiscono. In tal senso, il titolare del trattamento dei dati a fronte del contenimento di costi dovrà comunque provvedere al salvataggio (backup) dei dati allocati nella cloud, ad esempio creandone una copia locale (eventualmente sotto forma di archivio compresso), allo scopo di gestire gli eventuali rischi insiti nell'acquisizione di servizi che, pur con i vantaggi dell'economicità, potrebbero tuttavia non offrire sufficienti garanzie di affidabilità e di disponibilità.

- **Selezionare i dati da inserire nella cloud**

Alcune informazioni che si intende inserire sui sistemi del fornitore di servizio, per loro intrinseca natura, quali ad esempio i dati sanitari, genetici, reddituali, biometrici o quelli coperti da segreto industriale, possono esigere particolari misure di sicurezza. In tali casi, poiché dal relativo inserimento nella cloud consegue comunque una attenuazione, seppur parziale, della capacità di controllo esercitabile dall'utente, ed una esposizione di tali informazioni a rischi non sempre prevedibili di potenziale perdita o di accesso non consentito, l'utente medesimo dovrebbe valutare con responsabile attenzione se ricorrere al servizio di cloud computing oppure mantenere in house il trattamento di tali tipi di dati.

- **Non perdere di vista i dati**

E' sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto anche verificando se i dati rimarranno nella disponibilità fisica dell'operatore proponente, oppure se questi svolga un ruolo di intermediario, ovvero offra un servizio progettato sulla base delle tecnologie messe a disposizione da un operatore terzo. Si pensi ad esempio a un applicativo in modalità cloud nel quale il fornitore del servizio finale (Software as a Service) offerto all'utente si avvalga di un servizio di stoccaggio dati acquisito da un terzo. In tal caso, saranno i sistemi fisici di quest'ultimo operatore che concretamente ospiteranno i dati immessi nella cloud dall'utente.

- **Informarsi su dove risiederanno, concretamente, i dati**

Sapere in quale Stato risiedono fisicamente i server sui quali vengono allocati i dati, è determinate per stabilire la giurisdizione e la legge applicabile nel caso di controversie tra l'utente e il fornitore del servizio. La presenza fisica dei server in uno Stato comporterà per l'autorità giudiziaria nazionale, infatti, la possibilità di dare esecuzione ad ordini di esibizione, di accesso o di sequestro, ove sussistano i presupposti giuridici in base al singolo ordinamento nazionale. Non è, quindi,

indifferente per l'utente sapere se i propri dati si trovino in un server in Italia, in Europa o in un imprecisato Paese extraeuropeo. In ogni caso, l'utente, prima di inserire i dati nella nuvola informatica, dovrebbe assicurarsi che il trasferimento tra i diversi paesi in cui risiedono le cloud avvenga nel rispetto delle cautele previste a livello di Unione europea in materia di protezione dei dati personali, che esigono particolari garanzie in ordine all'adeguatezza del livello di tutela previsto dagli ordinamenti nazionali per tale tipo di informazioni.

- **Attenzione alle clausole contrattuali**

Una corretta e oculata gestione contrattuale può supportare sia l'utente, sia il fornitore nella definizione delle modalità operative e dei parametri di valutazione del servizio, oltre a individuare i parametri di sicurezza necessari per la tipologia di attività gestita. In ogni caso, è importante valutare l'idoneità delle condizioni contrattuali per l'erogazione del servizio di cloud con riferimento ad obblighi e responsabilità in caso di perdita, smarrimento dei dati custoditi nella nuvola e di conseguenze in caso di decisione di passaggio ad altro fornitore. Costituiscono elementi
da privilegiare la previsione di garanzie di qualità chiare, corredate da penali che pongano a carico del fornitore eventuali inadempienze o le conseguenze di determinati eventi (es. accesso non consentito, perdita dei dati, indisponibilità per malfunzionamenti, ecc.). Si suggerisce, inoltre, di verificare eventuali soggetti terzi delegati alla fornitura di servizi intermedi e che concorrono all'erogazione del servizio finale rivolto all'utente, ovvero la preventiva identificazione dei diversi fornitori successivamente coinvolti nel trattamento. Si raccomanda, infine, di accertare quale sia la quantità di traffico dati prevista dal contratto oltre la quale vengono addebitati oneri economici supplementari.

- **Verificare le politiche di persistenza dei dati legate alla loro conservazione**

In fase di acquisizione del servizio cloud è opportuno approfondire le politiche adottate dal fornitore, che si dovrebbero poter evincere dal contratto, relative ai tempi di persistenza dei dati nella nuvola. Da una parte l'utente dovrebbe accertare il termine ultimo, successivo alla scadenza del contratto, oltre il quale il fornitore cancella definitivamente i dati che gli sono stati affidati. Dall'altra, il fornitore dovrà presentare adeguate garanzie, assicurando che i dati non saranno conservati oltre i suddetti termini o comunque al di fuori di quanto esplicitamente stabilito con l'utente stesso. In ogni caso, i dati dovranno essere sempre conservati nel rispetto delle finalità e delle modalità concordate, escludendo duplicazioni e comunicazioni a terzi.

- **Esigere e adottare opportune cautele per tutelare la confidenzialità dei dati**

Nell'ottica di proteggere la confidenzialità dei propri dati, l'utente dovrebbe valutare anche le misure di sicurezza utilizzate dal fornitore per consentire l'allocazione dei dati nella cloud. In generale si raccomanda di privilegiare i fornitori che utilizzano a tal fine tecniche di trasmissione sicure, tramite connessioni cifrate (specie quando i dati trattati sono informazioni personali o comunque dati che devono restare riservati), coadiuvate da meccanismi di identificazione dei soggetti autorizzati all'accesso, la cui complessità sia commisurata alla criticità dei dati stessi. Nella maggior parte dei casi risulta adeguato l'utilizzo di semplici meccanismi di identificazione, basati su username e password, purché le password non siano banali e vengano scelte di lunghezza adeguata. Nell'ipotesi in cui il trattamento riguardi particolari tipologie di dati - quali quelli sanitari, genetici, reddituali e biometrici o, più in generale, dati la cui riservatezza possa considerarsi "critica" - si raccomanda oltre all'utilizzo di protocolli sicuri nella fase di trasmissione, anche la conservazione in forma cifrata sui sistemi del fornitore di servizio.

- **Formare adeguatamente il personale**

Il personale preposto al trattamento di dati attraverso i servizi di cloud computing dovrebbe essere sottoposto a specifici interventi formativi, che evidenzino adeguatamente le modalità più idonee per l'acquisizione e l'inserimento dei dati nella cloud, la consultazione e in generale l'utilizzo dei nuovi servizi esternalizzati e delle indicazioni sin qui illustrate, allo scopo di mitigare rischi per la protezione dei dati derivanti non solo da eventuali comportamenti sleali o fraudolenti, ma anche causati da errori materiali, leggerezza o negligenza: circostanze queste che potrebbero dare luogo ad accessi illeciti, perdita di dati o, più in generale, trattamenti non consentiti.

Capitolo VI
30 giugno 2014: il deposito telematico di atti e documenti diventa obbligatorio

Sommario: 6.1. Art. 16 bis decreto legge 18.10.12 n. 179, introdotto dalla Legge di Stabilità 2013. – 6.2. Obbligo per l'avvocato di deposito telematico di atti di terzi. – 6.3. Il momento perfezionativo del deposito di atti telematici. – 6.4. Le comunicazioni telematiche di cancelleria nel civile e nel penale dopo il decreto legge 18 ottobre 2012 n. 179.

6.1. - Art. 16 bis decreto legge 18.10.12 n. 179, introdotto dalla Legge di Stabilità 2013.

Abbiamo visto, nel capitolo III, come il decreto del Ministero della Giustizia che riconosceva, in un determinato Ufficio Giudiziario, il VALORE LEGALE del deposito telematico dell'atto o del documento, consentiva al professionista di depositare telematicamente il proprio atto o documento nel rispetto del c.p.c. senza la necessità di depositare anche il documento cartaceo.
Fino al 29 giugno 2014, anche in presenza del riconoscimento del valore legale del deposito telematico, sarà sempre possibile effettuare il deposito dell'atto nella forma tradizionale e quindi mediante il solo deposito cartaceo in Cancelleria ma l'art. 16 bis del decreto legge del 18 ottobre 2012 n. 179, introdotto dalla Legge di Stabilità 2013[11], prevede dal **30 giugno 2014**, **l'obbligatorietà del deposito telematico degli atti e dei documenti "da parte dei difensori delle parti precedentemente costituite … 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".**
Il medesimo articolo prevede inoltre l'**obbligatorietà del deposito telematico anche per il procedimento d'ingiunzione**, escluso però (in quanto atto introduttivo) il giudizio di opposizione.
Dal 30 giugno 2014, in tutti i Tribunali, la regola sarà quella del deposito telematico di atti e documenti nei seguenti procedimenti:
- **procedimenti civili, contenziosi, volontaria giurisdizione**
- **processi esecutivi**
- **procedure concorsuali ***
- **procedimento di ingiunzione**

A riguardo delle **procedure concorsuali**, l'art. 16 bis del decreto legge del 18 ottobre 2012 n. 179, introdotto dalla Legge di Stabilità 2013, dispone l'obbligatorietà del deposito telematico degli atti e dei documenti solo **"da parte del curatore, del commissario giudiziale, del liquidatore, del commissario liquidatore e del commissario straordinario".**
Il citato articolo altresì prevede al numero 6 che "**negli uffici giudiziari diversi dai Tribunali (Giudice di Pace, Corte d'Appello, Corte di Cassazione) l'obbligo del deposito telematico decorre dal quindicesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale della Repubblica italiana dei decreti adottati ai sensi dell'art. 16-bis comma V, d.l. 179/2012 conv. in l. 221/2012.**

Senza esagerare ritengo che l'art. 16 bis sia una vera e propria rivoluzione per il processo telematico in quanto, per la prima volta, il legislatore pone un vero e proprio divieto normativo per il deposito di atti e documenti con la forma tradizionale, quella cartacea.

[11] http://www.altalex.com/index.php?idnot=19440

Rilevo però come la norma stessa, pur obbligando le parti al deposito telematico di atti e documenti, non sia esente da imperfezioni tali da compromettere realmente i vantaggi di un simile sistema di deposito degli atti.
Infatti, dall'attenta lettura dell'art. 16 bis si evince che l'obbligo del **deposito telematico riguarderebbe solo ed esclusivamente gli atti e documenti depositati dalle parti precedentemente costituite**.
Rimarrebbe quindi sempre possibile depositare il cartaceo non solo per la parte che deve instaurare il giudizio con atto di citazione o ricorso ma anche per la parte che, in un giudizio incardinato, deve costituirsi per conto del proprio assistito.
Sul punto bisogna dire che la norma potrebbe apparire coerente per l'esclusione del deposito telematico dell'atto di citazione (e quindi dell'iscrizione a ruolo telematica) in quanto ad oggi tale deposito è stato sperimentato solo in qualche Tribunale se non fosse per il fatto che il Ministero della Giustizia ha però ben regolamentato tale tipo di deposito[12]; discorso a parte merita la comparsa di costituzione e risposta che, al contrario, non solo è anch'essa riconosciuta dal Ministero della Giustizia e DGSIA come tipologia di atto depositabile telematicamente[13] ma è presente (quale tipologia di atto depositabile) in tutti i Tribunali nei quali è possibile depositare a valore legale atti e documenti.
Aggiungo che, a mio avviso, la "quadratura del cerchio" e la piena convenienza dell'avvocato nell'utilizzo del PCT è proprio individuabile nel deposito telematico di questi due atti: citazione e ricorso e comparsa di costituzione in giudizio in quanto potrebbero consentire sia di prendere visione sia di fare il download sul proprio computer di tutti i documenti depositati dall'altra parte.
Se le cose restassero così, l'avvocato della parte che deve costituirsi in giudizio dovrebbe comunque recarsi in cancelleria almeno due volte: la prima per estrarre copia dei documenti depositati da parte attrice o ricorrente e la seconda al momento della costituzione in giudizio.
E' anche vero che è DOVERE DELLA CANCELLERIA inserire nel fascicolo informatico le copie informatiche di atti e documenti quando questi siano stati depositati su supporto cartaceo (art. 11 specifiche tecniche del 18 LUGLIO 2011 – fascicolo informatico – così come previste dall'art. 34 del D.M. 44/2011 che, a sua volta, prevede per la cancelleria il medesimo adempimento all'art. 9) ma onestamente ritengo alquanto improbabile che, tempestivamente, la cancelleria riesca a scansionare tutti gli atti e documenti cartacei depositati dalla parte al momento dell'iscrizione a ruolo della causa o della costituzione in giudizio.
Auspico, quindi, in attesa di modifica normativa, l'applicazione di prassi dettate dal buon senso al fine non vedere in gran parte compromesso il beneficio previsto dall'art. 16 ter con l'obbligo del deposito telematico; una soluzione (fino alla modifica della norma) potrebbe essere quella adottata presso i Tribunali Amministrativi Regionali dinanzi ai quali l'avvocato, già da molto tempo, è obbligato non solo a depositare atti e documenti in forma cartacea ma anche su supporto informatico (CD-ROM o DVD), attestando naturalmente la conformità dei documenti digitali inseriti nel supporto informatico a quella dei documenti depositati in forma cartacea; credo però che questa procedura non sia percorribile con l'attuale sistema. Per tale motivo ho ideato e testato con successo, presso il Tribunale di Teramo, una procedura di deposito utilizzando le funzioni PCT ad oggi disponibili che consente il deposito telematico dell'atto introduttivo e dei documenti dopo il deposito degli stessi nella forma tradizionale.

[12] http://pst.giustizia.it/PST/it/pst_1_0.wp?previousPage=pst_1_12&contentId=SPR377

[13] http://www.processotelematico.giustizia.it/pdapublic/resources/Elenco%20atti%20PCT%20cognizione%2020-10-2010.pdf

Utilizzando questa procedura, pur avvenendo il deposito dell'atto di citazione o del ricorso nel rispetto dell'art. 16 bis, la cancelleria, accettando la busta telematica pervenuta dall'attore, si troverebbe sul proprio sistema informatico (SICID), consultabile dai professionisti attraverso il POLISWEB, i file's contenenti la riproduzione digitale dei documenti cartacei depositati.
Così operando, il difensore della parte convenuta, potrebbe fare a meno di recarsi in cancelleria e di estrarre copia dei documenti depositati al momento dell'iscrizione della causa a ruolo potendo consultare e fare il download degli stessi attraverso il POLISWEB e potrebbe poi costituirsi telematicamente evitando quindi, anche per tale adempimento, di recarsi fisicamente in cancelleria.

6.2. – Obbligo per l'avvocato di deposito telematico di atti di terzi.

L'art. 16 bis prevede inoltre che "…**le parti provvedono, con le modalità di cui al presente comma, a depositare gli atti e i documenti provenienti dai soggetti da esse nominati".**
Ciò significa che sarà obbligo dell'avvocato depositare telematicamente non solo gli atti di sua produzione ma anche quelli, ad esempio, dei C.T.P. (consulenti tecnici di parte) i quali, nominati dal proprio assistito nel corso del procedimento con il compito di affiancare il Consulente nominato dal Giudice, provvederanno a consegnare al professionista il loro elaborato affinché possa essere depositato telematicamente da quest'ultimo.

6.3. – Il momento perfezionativo del deposito di atti telematici.

E' fondamentale per il professionista, al fine di non incorrere in decadenze, conoscere quale sia il momento in cui si perfezioni il deposito telematico dell'atto o del documento.
L'Art. 16 ter n. 7, stabilisce che "**Il deposito si ha per avvenuto nel momento in cui viene generata (e ricevuta dal professionista) la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del Ministero della Giustizia".**
La lettura di tale articolo sembrerebbe autorizzare l'avvocato al deposito del proprio atto in qualsiasi ora del giorno, ad esempio, della scadenza dello stesso, ponendo come unica condizione che la ricevuta di consegna, rilasciata dal gestore di posta elettronica certificata del Ministero della Giustizia, arrivi entro e non oltre le 23.59.
In realtà tale norma deve essere letta e raccordata con quella prevista (e non abrogata) dall'art. 13 del D.M. 21.02.2011 n. 44 la quale se è vero che al numero 2 prevede la stessa ipotesi prevista dall'art. 16 ter n. 7, al n. 3 prevede che "**Quando la ricevuta è rilasciata dopo le ore 14 il deposito si considera effettuato il giorno feriale immediatamente successivo**.
Per tale motivo è possibile affermare che, purtroppo, qualora il professionista attenda l'ultimo giorno utile per effettuare il deposito telematico dell'atto o del documento debba farlo avendo cura di rispettare l'orario delle ore 14.00 affinché entro tale ora possa giungere la ricevuta di consegna rilasciata dal gestore di posta certificata del Ministero della Giustizia.
Ove il deposito avvenisse alle 13,58 dell'ultimo giorno utile per effettuarlo e la ricevuta di consegna giungesse alle 14.01 ne conseguirebbe il deposito fuori termine in quanto lo stesso verrebbe si considerato depositato ma nel giorno feriale immediatamente successivo.
A mio avviso, con la formulazione del n. 7 dell'art. 16 ter, il legislatore aveva nelle sue intenzioni, quella di eliminare la previsione indicata nel n. 3 dell'art. 13 del D.M. 21.02.2011 n. 44 ma, non avendo disposto l'abrogazione di quest'ultima, ha fallito nel suo intento.
Consiglio quindi ai colleghi di depositare i loro atti telematicamente o nel pomeriggio del giorno precedente alla scadenza dello stesso o entro le ore 12.00 del giorno della scadenza.

Dal novembre 2011 deposito telematicamente i miei atti nei Tribunali ove tale deposito ha valore legale e, a dire il vero, ad oggi posso confermare che le ricevute di spedizione e consegna del deposito telematico giungono a pochi secondi dall'avvenuto deposito.
L'avvocato dovrà quindi evitare di depositare telematicamente in prossimità delle ore 14.00 del giorno di scadenza in quanto, ove la ricevuta di consegna giungesse dopo le ore 14.00 ben difficilmente potrebbe ottenere dal Giudice la rimessione in termini e ciò proprio per il disposto del n. 3 dell'art. 13 del D.M. 21.02.2011 n. 44.
Al contrario, ove depositasse telematicamente con congruo anticipo (nel pomeriggio del giorno precedente alla scadenza dello stesso o entro le ore 12.00 del giorno della scadenza) e ove, ciò nonostante, la ricevuta di consegna venisse consegnata dopo le ore 14.00 potrebbe sicuramente rivolgersi al Giudice formulando istanza ex art. 153 secondo comma c.p.c. il quale dispone che "la parte che dimostra di essere incorsa in decadenze per causa ad essa non imputabile può chiedere al giudice di essere rimessa in termini".

6.4. – Le comunicazioni telematiche di cancelleria nel civile e nel penale.

Il decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla L. 17 dicembre 2012 n. 221, ha innovato profondamente anche a riguardo delle comunicazioni (biglietti) telematiche di cancelleria sia nei procedimenti civili che penali.
Prima di tale norma, la materia era regolata dall' art. 51 D.L. 112/2008, modificato dalla Legge 22.02.2010 n. 24 e dall' art. 35 D.M. 44/2011 e 136 c.p.c. così come modificato dalla L. 183/11 in vigore dal 01.02.2012.
Analizziamo le disposizioni più importanti introdotte dal decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni dalla L. 17 dicembre 2012 n. 221.

Art.16 decreto-legge 18 ottobre 2012, n. 179
(Biglietti di cancelleria, notificazioni e comunicazioni per via telematica)

4. *Nei* ***procedimenti civili*** *le comunicazioni e le notificazioni a cura della cancelleria sono effettuate esclusivamente per via telematica all'indirizzo di posta elettronica certificata risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni, secondo la normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici.*

Nei procedimenti civili quindi si attesta come mezzo ufficiale e primario per la comunicazione ai difensori dei biglietti di cancelleria quello della posta elettronica certificata.
Sul punto segnalo massima attenzione in quanto molti colleghi sono convinti che l'indirizzo per ricevere le comunicazioni a mezzo PEC dalla cancelleria sia quello inserito nell'atto; ma così non è in quanto la norma sul punto è chiara nell'affermare che l'indirizzo PEC al quale la cancelleria inoltrerà le comunicazioni a mezzo PEC è quello risultante da PUBBLICI ELENCHI e quindi, per i professionisti, quello risultante dal REGINDE (Registro Generale Indirizzi Elettronici) gestito e tenuto dal Ministero della Giustizia ed alimentato o singolarmente dai professionisti iscritti in albi o dagli Ordini professionali con la procedura come meglio descritta nel capitolo 4.2.5.
Affinchè l'Ordine professionale possa procedere è naturalmente necessario che allo stesso il professionista abbia cura di comunicare il proprio indirizzo di posta elettronica certificata.

Art. 16 decreto-legge 18 ottobre 2012, n. 179
(Biglietti di cancelleria, notificazioni e comunicazioni per via telematica)

6. *Le notificazioni e comunicazioni ai soggetti per i quali la legge prevede l'obbligo di munirsi di un indirizzo di posta elettronica certificata, che non hanno provveduto ad istituire o comunicare il predetto indirizzo,* ***sono eseguite esclusivamente mediante deposito in cancelleria****. Le stesse modalità si adottano nelle ipotesi di mancata consegna del messaggio di posta elettronica certificata per cause imputabili al destinatario.*

Tale disposizione ricalca, nei suoi effetti pratici, quanto già previsto dall'art. 51 D.L. 112/2008, modificato dalla Legge 22.02.2010 n. 24 prevedendo IL DEPOSITO IN CANCELLERIA della comunicazione ove il professionista non abbia provveduto ad istituire o comunicare l'indirizzo di posta elettronica certificata; in altri termini, il professionista inadempiente, rischierà di non conoscere mai il contenuto di quella comunicazione o di conoscerla quando, ormai ad esempio, sarà spirato il termine entro il quale avrebbe dovuto eseguire un determinato adempimento.
Ma le stesse conseguenze si avranno anche nel caso in cui la cancelleria, dopo aver inviato la comunicazione telematica alla PEC del professionista, riscontri la mancata consegna dello stesso messaggio PER CAUSE IMPUTABILI AL DESTINATARIO.
Sul punto è opportuno evidenziare quali siano i casi in cui, pur avendo il professionista un valido indirizzo di posta elettronica certificata, possa verificarsi una mancata consegna del messaggio inviato dalla cancelleria per causa allo stesso imputabile.
Ciò potrebbe verificarsi nei seguenti casi:
- il professionista è dotato di PEC ma non ha comunicato al proprio Ordine il relativo indirizzo;
- il professionista è dotato di PEC, ha comunicato al proprio Ordine il relativo indirizzo ma non ha mai attivato e resa operativa la PEC;
- il professionista è dotato di PEC, ha comunicato al proprio Ordine il relativo indirizzo ma, nella comunicazione ha inserito in maniera imprecisa l'indirizzo della PEC;
- il professionista è dotato di PEC, ha comunicato al proprio Ordine il relativo indirizzo ma ha successivamente attivato altro indirizzo PEC senza comunicare la variazione al proprio Ordine;
- il professionista è dotato di PEC, ha comunicato al proprio Ordine il relativo indirizzo ma la sua casella PEC ha raggiunto il limite massimo di messaggi ricevibili;
- il professionista è dotato di PEC, ha comunicato al proprio Ordine il relativo indirizzo ma l'Ordine, nel predisporre l'invio del file xml al Ministero della Giustizia per l'alimentazione del REGINDE ha inserito nello stesso in modo impreciso l'indirizzo PEC del professionista.

In tutti i casi sopra elencati, fatta eccezione per l'ultimo, il professionista incorrerebbe nella previsione prevista dalla norma e quindi la mancata ricezione si avrebbe per una causa imputabile allo stesso.
Nell'ultima ipotesi, a mio avviso, essendo la mancata ricezione imputabile all'Ordine e non al professionista quest'ultimo potrebbe avanzare istanza ex art. 153 secondo comma c.p.c. il quale dispone che "la parte che dimostra di essere incorsa in decadenze per causa ad essa non imputabile può chiedere al giudice di essere rimessa in termini".

Art. 16 decreto-legge 18 ottobre 2012, n. 179
(Biglietti di cancelleria, comunicazioni e notificazioni per via telematica)

Dal 15/10/2013: *le comunicazioni e notificazioni a cura della cancelleria* ***anche a destinatari diversi dai difensori (CTU, parti)*** *si* ***eseguono esclusivamente in via telematica ove rinvenuto l'indirizzo PEC del destinatario in pubblici elenchi.***

Art. 16 decreto-legge 18 ottobre 2012, n. 179

(Biglietti di cancelleria, comunicazioni e notificazioni per via telematica)

Nei **procedimenti penali** dinanzi ai **tribunali e alle corti di appello** le notificazioni a persona diversa dall'imputato a norma degli articoli 148, comma 2-bis, 149, 150 e 151, comma 2, del codice di procedura penale sono effettuate esclusivamente per via telematica all'indirizzo di posta elettronica certificata risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni … ***a decorrere dal 15 dicembre 2014.***

La norma sopra trascritta prevede anche per i procedimenti penali, relativamente alle comunicazioni da parte della cancelleria, la stessa situazione più sopra analizzata e descritta per i procedimenti civili ma ciò solo dal 15 dicembre 2014.
Evidenzio come in alcuni Uffici Giudiziari le comunicazioni telematiche nel settore penale siano già attive o con valore legale o in corso di sperimentazione (doppio binario):

TRIBUNALE E PROCURA DELLA REPUBBLICA TORINO
Dal 1° ottobre 2012 valore legale* comunicazioni telematiche nel settore penale.
***ex art. 51 DL 25.06.2008 n. 112 e succ. mod.**

CORTE DI APPELLO BOLOGNA
Dal 13 gennaio 2013 avvio fase sperimentale comunicazioni telematiche nel settore penale.

CORTE DI APPELLO GENOVA
Dal 03 giugno 2013 avvio fase sperimentale comunicazioni telematiche nel settore penale.

BARI
avvio fase sperimentale comunicazioni telematiche nel settore penale:

TRIBUNALE DI SORVEGLIANZA: 05 novembre 2012
PROCURA REPUBBLICA TRIBUNALE: 12 novembre 2012
CORTE DI APPELLO: 19 febbraio 2013
TRIBUNALE MINORENNI: 15 marzo 2013

Art. 16 decreto-legge 18 ottobre 2012, n. 179
(Biglietti di cancelleria, comunicazioni e notificazioni per via telematica)

8. *Quando non è possibile procedere ai sensi del comma 4 per causa non imputabile al destinatario, nei procedimenti civili si applicano l'articolo 136, terzo comma, e gli articoli 137 e seguenti del codice di procedura civile e, nei procedimenti penali, si applicano gli articoli 148 eseguenti del codice di procedura penale.*

La norma prevede l'ipotesi in cui la comunicazione di cancelleria non possa essere inviata telematicamente per causa non imputabile al destinatario e quindi causa un problema tecnico dei sistemi informatici della cancelleria o del Gestore Centrale dei sistemi informativi del Ministero della Giustizia.
In questi casi si tornerà al vecchio sistema e quindi alla notifica cartacea per il tramite dell'ufficiale giudiziario o a mezzo fax.

Art. 16 decreto-legge 18 ottobre 2012, n. 179
(Biglietti di cancelleria, comunicazioni e notificazioni per via telematica)

14. *All'articolo 40 del testo unico delle disposizioni legislative e regolamentari in materia di spese di giustizia, di cui al decreto del Presidente della Repubblica 30 maggio 2002, n. 115, dopo il comma 1 -bis è aggiunto, in fine, il seguente: «1 - ter.* ***L'importo del diritto di copia, aumentato di dieci volte, è dovuto per gli atti comunicati o notificati in cancelleria nei casi in cui la comunicazione o la notificazione al destinatario non si è resa possibile per causa a lui imputabile.».***

La norma in questione si applica nel caso in cui il professionista, non raggiunto dalla comunicazione telematica di cancelleria per causa allo stesso imputabile, richiederà ottenere copia della comunicazione cartacea depositata in cancelleria; potrà farlo a condizione che paghi il diritto di copia aumentato di dieci volte.
Sul punto ritengo superfluo ogni commento.

Capitolo VII
Deposito telematico: le regole, gli eventi successivi e le problematiche irrisolte

Sommario: Premessa - 7.1. Il formato dell'atto e dei documenti da depositare telematicamente. – 7.2. Gli eventi successivi al deposito telematico. – 7.2.1 La ricevuta di accettazione. – 7.2.2 La ricevuta di avvenuta consegna. - 7.2.3 La ricevuta esiti controlli automatici. - 7.2.4 La ricevuta di acquisizione, da parte del cancelliere, dell'atto e/o documento. - 7.3. Mandato congiunto, cancellerie e deposito telematico. - 7.4. Comparsa di costituzione e deposito telematico. - 7.5. Comparsa di costituzione, mandato congiunto e deposito telematico. - 7.6. Le problematiche irrisolte.

Premessa.
In questo capitolo cercherò di spiegare da una parte, le regole da seguire per effettuare telematicamente il deposito di atti e documenti e, dall'altra, gli eventi riscontrabili dopo il deposito.

7.1. – Il formato dell'atto e dei documenti da depositare telematicamente.

Le regole tecniche vigenti impongono al professionista di osservare, scrupolosamente, quanto dalle stesse dettato affinché l'atto o il documento da depositare telematicamente venga accettato dalla struttura informatica del Ministero della Giustizia.
A tale scopo dobbiamo distinguere tra deposito dell'atto predisposto dal professionista e deposito del documento.
Quanto al primo, il professionista potrà redigerlo con il tradizionale programma di video scrittura utilizzato; una volta così predisposto l'atto, dovrà trasformarlo nel formato **PDF TESTO** senza utilizzare lo scanner.
Chi usa Open Office, può creare il file pdf cliccando sul tasto **"pdf"** presente nella barra degli strumenti; chi usa Word 2010 può salvare l'atto in formato PDF utilizzando la funzione presente in **"salva con nome"**, chi invece usa altri programmi che non consentono quanto sopra indicato **può "stamparla in pdf" con stampante virtuale** usando, ad esempio, il programma gratuito "**PDF CREATOR**" o **"PDF24"** o similari; è necessario, naturalmente, verificare di aver installato sul proprio computer una **stampante virtuale PDF (**"**PDF CREATOR**" o **"PDF24"** o similari**)**. Dal menu **FILE > STAMPA > selezionare la stampante PDF > OK > salvare il file PDF in qualsiasi cartella del computer.**
Una volta trasformato l'atto in PDF TESTO lo stesso dovrà essere FIRMATO DIGITALMENTE dal professionista. Sul punto segnalo che i software ad oggi a disposizione per depositare telematicamente atti e documenti consentono l'apposizione della firma digitale anche nella fase successiva e comunque prima dell'invio della "busta telematica" nella quale l'atto viene inserito.
Una domanda che spesso ricorre è la seguente: quali sono gli atti da firmare digitalmente? Suggerisco al professionista di apporre la firma digitale su ogni atto nel quale avrebbe apposto la firma autografa.
I **documenti cartacei** da depositare telematicamente **dovranno essere trasformati**, mediante scanner, **in file PDF IMMAGINE (ad ogni documento dovrà corrispondere un file PDF avente quale nome quello del documento;** la denominazione del file non dovrà contenere caratteri speciali come lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").
Non è necessario sottoscrivere i documenti con firma digitale a meno che ciò non sia richiesto dalla tipologia del documento.

Considerando che le regole tecniche prevedono che la "busta telematica" non possa avere un peso superiore a 30 MB, suggerisco di scansionare i documenti **IN BIANCO E NERO** e a **BASSA RISOLUZIONE** (100 dpi ritengo posso essere una risoluzione ottimale).
Non vado oltre nella spiegazione in quanto, una volta predisposti come descritto i file's contenenti l'atto e i documenti da depositare, i passaggi successivi sono diversi a seconda del software utilizzato (tecnicamente chiamato redattore atti) per la creazione della "busta telematica" (secondo le specifiche tecniche definite nel provvedimento del 18 luglio 2011) all'interno della quale verranno inseriti l'atto e/o i documenti da depositare telematicamente prima che la stessa venga trasmessa tramite PEC alla PEC dell'Ufficio Giudiziario.

7.2. – Gli eventi successivi al deposito telematico.

Successivamente alla trasmissione telematica del proprio atto e/o documento il professionista dovrà controllare la propria casella di posta elettronica certificata in quanto, per ogni trasmissione telematica gli verranno inviate (ove la procedura sia stata effettuata correttamente) nel seguente ordine, quattro ricevute:

1) RICEVUTA DI ACCETTAZIONE

2) RICEVUTA DI AVVENUTA CONSEGNA

3) RICEVUTA ESITI CONTROLLI AUTOMATICI

4) RICEVUTA DI ACQUISIZIONE, DA PARTE DEL CANCELLIERE, DELL'ATTO E/O DOCUMENTO.

7.2.1 – La ricevuta di accettazione.

E' la ricevuta rilasciata dal gestore della PEC del professionista ed **attesta la spedizione** di quanto inviato alla PEC dell'Ufficio Giudiziario a cui l'atto e/o il documento è stato inviato ai fini del deposito telematico.

7.2.2 – La ricevuta di avvenuta consegna.
E' la ricevuta rilasciata dal gestore della PEC dell'Ufficio Giudiziario ed **attesta l'avvenuta consegna** di quanto inviato dalla PEC del professionista ai fini del deposito telematico.
Tale ricevuta attesta il momento perfezionativo del deposito telematico e ciò ai sensi e per gli effetti dell'art. 16 ter n. 7 decreto legge 18.10.12 n. 179, introdotto dalla Legge di Stabilità 2013 il quale, come abbiamo visto nel precedente capitolo, stabilisce che "**Il deposito si ha per avvenuto nel momento in cui viene generata (e ricevuta dal professionista) la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del Ministero della Giustizia".**
Contiene in allegato il messaggio inviato dal professionista oltre alla data e ora del deposito e un codice univoco di identificazione del messaggio inviato.
Inutile sottolineare come tale ricevuta debba essere conservata scrupolosamente dal professionista in quanto, ove si renda necessario, costituisce il modo per fornire la prova dell'avvenuto deposito.

7.2.3 – La ricevuta esiti controlli automatici.
E' la ricevuta proveniente dal computer (server) della cancelleria alla quale l'atto e/o il documento è stato spedito all'interno della busta telematica; il software del Ministero della Giustizia, presente

nel server della cancelleria, procede all'esame della busta telematica effettuando i seguenti controlli: tipologia dei file's relativi all'atto e/o ai documenti depositati, verifica dell'esistenza in quell'ufficio giudiziario di un fascicolo con lo stesso numero di ruolo indicato dal professionista; verifica che il detto fascicolo sia riconducibile al professionista che ha effettuato il deposito attraverso la corrispondenza del codice fiscale.
Attenzione: non sempre la ricezione di esito negativo dei controlli automatici equivale ad un invio telematico errato o non conforme alle regole tecniche; ad esempio, nel deposito telematico di una comparsa di costituzione e risposta (atto con il quale la parte si costituisce in giudizio) pur avendo seguito la corretta procedura e quindi il rispetto delle regole tecniche, la relativa ricevuta dei controlli automatici conterrebbe esito negativo in quanto il software ministeriale, nel verificare se il codice fiscale dell'avvocato che ha effettuato il deposito sia presente nel fascicolo in cui il deposito deve essere effettuato, non trovando rispondenza tra il codice fiscale dell'avvocato e quello presente nel fascicolo, non potrà che generare l'esito negativo dei controlli.
In questo caso sarà possibile leggere testo della ricevuta, oltre al tipo di errore rilevato dal sistema, anche il seguente avviso: **"sono necessarie verifiche da parte della cancelleria"**.

7.2.4 – La ricevuta di acquisizione, da parte del cancelliere, dell'atto e/o documento.

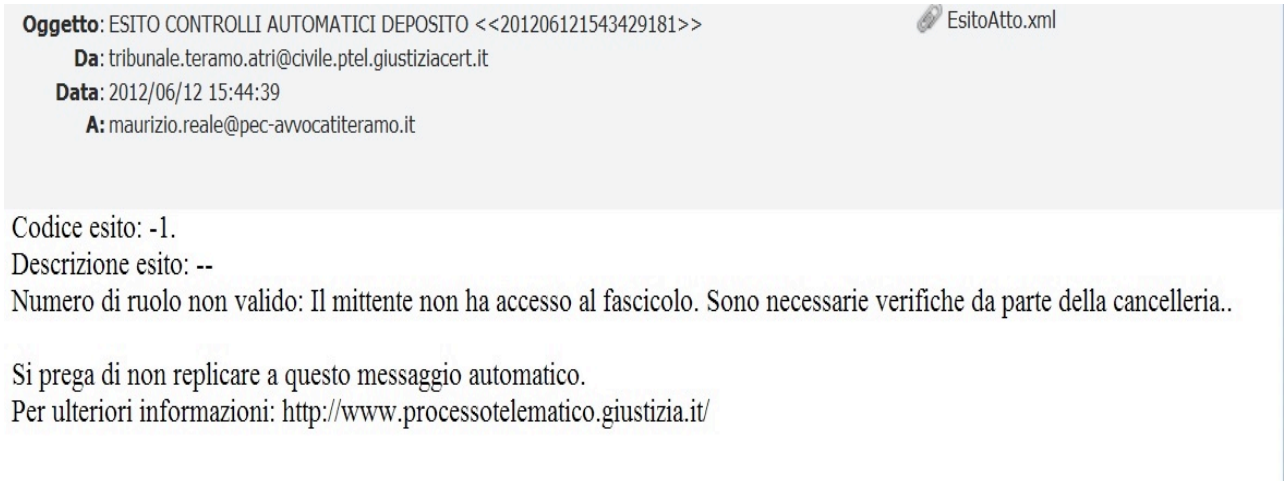
Le prime tre ricevute vengono inviate automaticamente, senza necessità di intervento manuale; la quarta ricevuta viene invece inoltrata "manualmente" dal cancelliere e attesta l'accettazione definitiva di quanto inviato telematicamente dal professionista. E' in questa fase che il cancelliere deve occuparsi di effettuare verifiche ove i controlli automatici abbiano dato esito negativo.
Nell'esempio descritto al punto precedente il cancelliere potrà visualizzare l'atto (comparsa di costituzione) e la procura alle liti al fine di verificare se l'avvocato abbia titolo per accedere a quel fascicolo; se la verifica è positiva il deposito telematico verrà definitivamente accettato mentre, in caso di esito negativo, verrà definitivamente respinto.

7.3 - Mandato congiunto, cancellerie e deposito telematico.

Nel caso di mandato congiunto i dati di entrambi i difensori devono essere inseriti nel SICID affinché gli stessi possano, ad esempio, relativamente a quel procedimento, ricevere le comunicazioni telematiche di cancelleria o depositare telematicamente atti.
L'esperienza maturata mi porta a rilevare che in diversi casi l'impiegato della cancelleria, nell'inserire i dati delle parti presenti nella nota iscrizione a ruolo, omette di inserire entrambi i nomi dei difensori limitandosi ad associare al fascicolo il solo nominativo di uno di loro (solitamente il primo).
Ciò comporta che l'avvocato escluso dall'inserimento, ove effettui un deposito telematico, otterrà (a seguito dei controlli automatici del software ministeriale) la ricevuta relativa ai detti controlli recante ESITO NEGATIVO nella quale si leggerà il seguente testo:

CODICE ESITO : -1
DESCRIZIONE ESITO: --
Numero di ruolo non valido: Il mittente non ha accesso al fascicolo. Sono necessarie verifiche da parte della cancelleria (FIG.01).

FIG.01:



E' vero che il cancelliere, solitamente, dinanzi a tale ESITO NEGATIVO, consultato il fascicolo cartaceo e verificato che in effetti l'avvocato risulta regolarmente difensore, accetta il deposito telematico dopo aver aggiunto, all'anagrafica SICID, i dati del predetto ma è altrettanto vero che ciò crea sicuramente PANICO nel professionista che incorre per la prima volta in una simile situazione.

7.4 - Comparsa di costituzione e processo telematico.

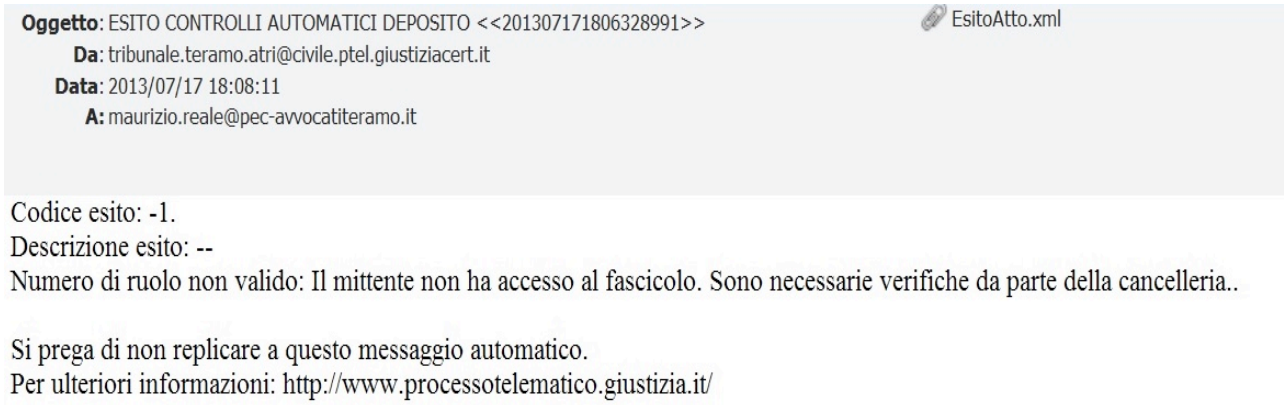
In riferimento a quanto riportato sia al precedente punto sia a proposito di quando scritto nel paragrafo 7.2.3, ove l'avvocato invierà telematicamente l'atto per la costituzione in giudizio, otterrà (a seguito dei controlli automatici effettuati dal software ministeriale) la ricevuta relativa ai detti controlli recante ESITO NEGATIVO nella quale si leggerà lo stesso testo di quello più sopra trascritto:

CODICE ESITO : -1

DESCRIZIONE ESITO: --

Numero di ruolo non valido: Il mittente non ha accesso al fascicolo. Sono necessarie verifiche da parte della cancelleria (FIG.02).

FIG.02:



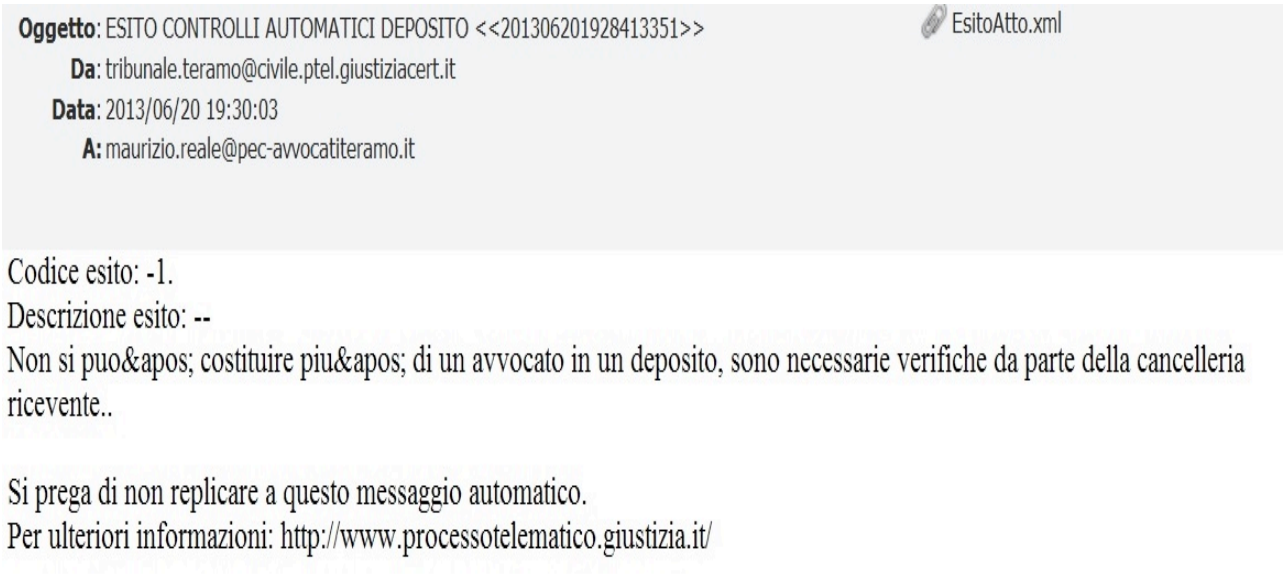
In questi casi il Cancelliere, dinanzi a tale ESITO NEGATIVO, esaminati i documenti allegati ed in particolare la procura alle liti e verificato che in effetti l'avvocato difende la parte convenuta,

accetta il deposito telematico dopo aver aggiunto, all'anagrafica SICID, i dati del predetto, associandolo quale difensore del convenuto.

7.5 - Comparsa di costituzione, mandato congiunto e processo telematico.

E' naturale che la parte possa conferire il mandato di rappresentanza a due professionisti.Qualsiasi redattore atti PCT consente di indicare, nella creazione del fascicolo telematico, anche il nominativo del secondo difensore.
In questo caso però, inviato telematicamente l'atto di costituzione l'avvocato otterrà (a seguito dei controlli automatici effettuati dal software ministeriale) la ricevuta relativa ai detti controlli recante ESITO NEGATIVO nella quale si leggerà il seguente testo:

CODICE ESITO : -1
DESCRIZIONE ESITO: --
Non si può costituire più di un avvocato in un deposito; sono necessarie verifiche da parte della cancelleria ricevente (FIG.03).
FIG.03:


Oggetto: ESITO CONTROLLI AUTOMATICI DEPOSITO <<201306201928413351>>
EsitoAtto.xml
Da: tribunale.teramo@civile.ptel.giustiziacert.it
Data: 2013/06/20 19:30:03
A: maurizio.reale@pec-avvocatiteramo.it

Codice esito: -1.
Descrizione esito: --
Non si puo' costituire piu' di un avvocato in un deposito, sono necessarie verifiche da parte della cancelleria ricevente..

Si prega di non replicare a questo messaggio automatico.
Per ulteriori informazioni: http://www.processotelematico.giustizia.it/

In questo caso il Cancelliere, dinanzi a tale ESITO NEGATIVO, esaminati i documenti allegati ed in particolare la procura alle liti e verificato che in effetti sono due gli avvocati nominati difensori dalla parte convenuta, accetterà il deposito telematico e aggiungerà, all'anagrafica SICID, i dati dei difensori; a volte è invece accaduto che il Cancelliere inserisca nell'anagrafica SICID solo i dati del primo difensore indicato e non anche quelli del secondo; così facendo l'avvocato escluso non potrà quindi accedere alle informazioni del fascicolo tramite il POLISWEB e non riceverà le comunicazioni telematiche di cancelleria a mezzo PEC fino a quando non avrà provveduto a far associare i suoi dati presenti nell'anagrafica SICID al fascicolo.

7.6 – Le problematiche (ad oggi) irrisolte.

Oltre a quelle sopra evidenziate altre problematiche, ad oggi irrisolte, "affliggono" i protagonisti del processo telematico, soprattutto nella fase successiva al deposito di atti e documenti.
7.6.1 – Atto depositato telematicamente e verifica (impossibile) della sottoscrizione digitale.

La prima problematica ha origine da quanto comunicato da DGSIA il 3 luglio 2013:

"l'operazione di Download Documento riportata al paragrafo 3.1 (Elenco consultazioni fascicolo informatico) della Documentazione Servizi Web v1.5 verrà modificata al fine di non consentire il download della copia originale del documento; si interverrà quindi sul parametro original. L'originale del documento informatico sarà disponibile quando verrà completato l'intervento relativo al rilascio telematico delle copie autentiche previo pagamento dei diritti dovuti. Rimarrà pertanto unicamente la possibilità di scaricare la versione PDF del documento privo della (eventuale) firma digitale. La modifica verrà rilasciata a breve e verrà installata sul territorio entro il 19 luglio prossimo"

Dalla lettura delle comunicazione risalta subito una colossale inesattezza (eufemisticamente parlando) in quanto parlare di copia e, addirittura, di "copia originale", relativamente ad un documento informatico, è un vero e proprio non senso!! Nel digitale non esiste nessuna differenza tra l'originale e copia, in quanto da un singolo documento posso riprodurre e replicare lo stesso all'infinito.
Quanto al contenuto del comunicato, dallo stesso si evince che tutti gli atti depositati telematicamente potranno essere visualizzati e "trasferiti" (tramite download da PDA) sul proprio PC in formato .pdf e non in formato .P7M (estensione questa tipica dei file firmati digitalmente).
Non sarà possibile quindi verificare, per avvocati e magistrati, "chi" e "quando" ha firmato digitalmente il file che troviamo nel fascicolo informatico con la conseguenza che, gli uni e gli altri (gli avvocati attraverso il "Polisweb" e i Magistrati tramite la "Consolle del Magistrato") dovranno affidarsi ai controlli automaticamente predisposti dal software ministeriale tra i quali è previsto quello di verificare che determinati file's, oltre che ad appartenere ad uno specifico tipo siano stati anche firmati digitalmente; la situazione, aggiunge DGSIA, potrà mutare "…**solo quando verrà completato l'intervento relativo al rilascio telematico delle copie autentiche previo pagamento dei diritti dovuti…"**.
Naturalmente, a intervento completato, l'avvocato, dovrà pagare i diritti (ammontanti a?) anche al solo fine di voler verificare, ad esempio, "chi" e "quando" ha firmato digitalmente quel file! Ciò equivale ad un vero e proprio obbligo "mascherato" da onere in quanto se è vero che, da una parte, nessuno obbligherà l'avvocato ad effettuare questa verifica (a pagamento) dall'altra non si deve dimenticare che tale apparente onere è in realtà, per il professionista, obbligo in quanto l'avvocato diligente e professionalmente attento alla tutela dei diritti del proprio assistito non potrà esimersi dal verificare (anche al fine di evitare procedimenti disciplinari per violazione al codice deontologico unitamente ad altri di natura risarcitoria) l'esistenza della firma digitale apposta nell'atto dall'avvocato di controparte e nella procura alle liti o addirittura la validità del certificato di sottoscrizione il quale potrebbe essere scaduto o stato revocato!
Mi limito ad evidenziare che la firma digitale assicura la genuinità del documento, la paternità dello stesso e la non ripudiabilità, così come disposto dall'art. 24 del Codice dell'Amministrazione Digitale:

Articolo 24
Firma digitale

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.

2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.
4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

L'articolo appena trascritto (e, conseguentemente, la necessità e il dovere per l'avvocato di operare i relativi controlli) assume un maggiore peso e rilevanza, ai fini della regolarità degli atti processuali depositati tramite PCT, se letto unitamente al disposto di cui all'art. 83 c.p.c. il quale impone al professionista e al magistrato la verifica dei requisiti formali normativamente richiesti per una regolare procura alle liti, la cui mancanza (di tali requisiti) potrebbe avere come conseguenza la nullità dell'atto!
Ma tale verifica è altresi fondamentale e assolutamente dovuta sotto il profilo legale, non solo per l'avvocato ma anche e soprattutto per il funzionario di cancelleria il quale, ad esempio, a seguito di decreto ingiuntivo telematico, rilascia, ai fini della notifica, copie cartacee conformi del ricorso dell'avvocato e del decreto del magistrato senza avere la concreta possibilità di verificare la genuinità e l'integrità dei rispettivi documenti e delle firme apposte; a ciò aggiungo che, nella maggior parte dei casi, la copia viene dichiarata conforme con la sintetica frase "è copia conforme all'originale" senza specificare, ad es. l'origine telematica del ricorso e del decreto e senza specificare attraverso quale procedimento sia stato possibile attestare che trattasi di copia conforme all'originale!
Mettiamoci nelle vesti dell'ingiunto e dell'avvocato al quale questi si rivolge: avrà tra le mani un ricorso per decreto ingiuntivo privo di qualsiasi firma e/o sottoscrizione autografa e qualora volesse verificare sia la genuinità e l'integrità del documento informatico originario (ricorso per decreto ingiuntivo, decreto del magistrato e firma di procura), sia le firme digitali apposte, oggi non potrebbe farlo mentre, domani (quando?) potrà farlo … pagando!
Stesso discorso si potrebbe fare per la costituzione in giudizio telematica e per tutti gli altri atti successivi con i quali la parte si potrà costituire telematicamente in giudizio.
E poi … pagare, pagare, pagare ma… in questo caso, per cosa? La domanda credo sia legittima in quanto il dipendente, pubblico ufficiale o funzionario di cancelleria che, nel rilascio di un determinato atto cartaceo materialmente, comunque, poneva in essere una determinata serie di attività mentre con il telematico nulla deve fare affinchè, tramite PDA, l'avvocato possa non solo visualizzare ma anche ottenere (tramite download sul proprio PC) la disponibilità dell'atto in formato digitale!
Al momento, quindi, nessuna delle parti potrà verificare "chi" e "quando" quel documento informatico ha firmato digitalmente e, fin quando le cose non cambieranno, dovremo affidarci e ci dovremo, quindi, fidare dei controlli automatici del PCT in fase di deposito della busta telematica contenente atto e documenti informatici da depositare nel fascicolo informatico.
Concludo con una piccola curiosità di cui sono direttamente testimone: tramite tutti i PDA già oggi sarebbe possibile richiedere il rilascio telematico delle copie autentiche e versare i diritti tramite pagamento telematico ma, inoltrata la richiesta, la stessa telematicamente arriva a destinazione (consolle cancelliere) ma il software attuale non consente però al cancelliere di evaderla; per farla breve: al momento …è possibile richiedere ma non è possibile ottenere risposta!

7.6.2 – Biglietto di cancelleria comunicato tramite PEC e verifica telematica (impossibile) del relativo esito.

Potrà sembrare strano ma ad oggi non è possibile, per l'avvocato, conoscere l'esito della comunicazione dei biglietti di cancelleria inviati tramite PEC ad altro avvocato o altra parte del processo: non è possibile quindi, tramite PDA, per l'avvocato, verificare se, ad es., la controparte abbia ricevuto (e in quale data) una determinata comunicazione.
Al momento, quindi, come si supera il problema?
Semplice … recandosi in cancelleria e chiedendo il rilascio di attestazione (cartacea) nella quale sia indicato l'esito della notifica.
Per cui … obbligo di deposito telematico, obbligo per il cancelliere di inoltrare il biglietto di cancelleria tramite PEC e … giusto per tornare alle origini, non perdere vecchie abitudini e continuare a perdere tempo… verifica, circa l'esito dello stesso, nel modo tradizionale ossia recandosi fisicamente in cancelleria!!
Il magistrato, relativamente a questa problematica, è più fortunato in quanto, tramite la sua "consolle", già oggi è in grado di verificare e conoscere l'esito della notifica.
Sembrerebbe, ma non ho conferme ufficiali sul punto, che DGSIA stia lavorando per rimediare a tale problematica: speriamo sia vero e, soprattutto, che il rimedio arrivi presto!

7.6.3 – Notifica tramite PEC ex L. 53/94 e (impossibile) deposito telematico dell'atto notificato presso l'Ufficio Giudiziario.

Sul punto rimando alla lettura del capitolo XII nel quale tratterò in maniera specifica le notifiche degli avvocati tramite la PEC ex L. 53/94 e nel quale meglio potrà effettuarsi la disamina della relativa e connessa problematica.

7.6.4 – Modalità del deposito del fascicolo telematico di parte di primo grado nel giudizio d'appello.

Lo spunto per questa riflessione mi è stato offerto dal collega e amico Mirco Minardi il quale, in un suo articolo[14], affronta il problema delle conseguenze relative al mancato deposito del fascicolo di parte del giudizio di primo grado nel giudizio di appello.
Lo scenario che si presenta è il seguente:
le parti del giudizio, in primo grado, soprattutto dal 30 giugno 2014, depositeranno il proprio fascicolo in una prima fase (costituzione in giudizio) nella maniera tradizionale e, successivamente, dovranno depositare telematicamente gli atti (e i documenti) successivi a quelli introduttivi (memorie ex art. 183 n. 6 c.p.c., eventuali memorie autorizzate dal Giudice, comparse conclusionali e repliche).
Il fascicolo risulterà quindi formato in parte dal cartaceo e in parte da file depositati tramite PCT o, per il convenuto che sin dall'inizio sia sia costituito telematicamente, solo da file depositati tramite PCT.
Come potrà il professionista depositare il proprio fascicolo di parte?
Nel caso di fascicolo di parte "misto" (cartaceo+digitale) potrebbe depositare solo la parte cartacea ma, la restante parte depositata tramite PCT come e chi la depositerà? Non potrà farlo

[14] http://www.lexform.it/giurisprudenza/diritto-processuale-civile/fascicolo-diritto-processuale-civile-giurisprudenza/giudizio-dappello-cosa-succede-se-non-viene-depositato-il-fascicolo-di-parte-di-primo-e-secondo-grado/

l'avvocato il quale non ha il "controllo" di quanto depositato, ad es., nel SICID e ad oggi, in mancanza di norma, non è previsto che il "trasferimento" del detto fascicolo alla cancelleria del Giudice di Appello debba avvenire da parte della cancelleria del Giudice di primo grado.
Le soluzioni ipotizzabili sono diverse ma ad oggi nessuna risulta essere stata adottata quale soluzione certa e definitiva.
Potrebbe ipotizzarsi che:
1) l'avvocato salvi sotto forma di file's tutte le ricevute complete di avvenuta consegna dei depositi effettuati nel corso del giudizio di primo grado ed alleghi le stesse al momento della costituzione (telematica) nel giudizio di Appello; ma ad oggi non tutte le Corti di Appello sono pronte e abilitate a ricevere telematicamente i depositi e, dinanzi a tale ulteriore ostacolo, sarebbe complicato anche per la cancelleria del Giudice di primo grado adempiere all'obbligo di trasmissione del fascicolo d'ufficio alla cancelleria del Giudice d'Appello;
2) l'avvocato proceda alla stampa delle ricevute di avvenuta consegna di tutti i depositi telematici effettuati nel corso del giudizio di primo grado, alla stampa dei relativi atti e documenti indicati in tali ricevute e attesti la conformità di tutti i documenti cartacei a quelli depositati telematicamente ma, il rilascio di tale conformità è ad oggi consentita per il professionista solo per le notifiche in proprio ex L. 53/94 ove non possa depositare tramite PCT il file "ricevuta di avvenuta consegna" in formato .eml (sul punto però vi sono altre problematiche che verranno esaminate le capitolo XIII e al quale rimando);
3) l'avvocato proceda come descritto al precedente punto facendosi però rilasciare la conformità da un pubblico ufficiale così come previsto dall'art. 23 del codice dell'amministrazione digitale.
E' assolutamente necessario che il legislatore colmi l'esistente vuoto normativo al fine di porre rimedio alla descritta e reale problematica.

Capitolo VIII
Revisione Geografia Giudiziaria e Processo Telematico

Sommario: Premessa - 8.1. Soppressione Uffici Giudiziari, SICID e Processo Telematico - 8.2. Soppressione Sezioni Distaccate di Tribunale e Processo Telematico - 8.3. Soppressione dei Tribunali Circondariali e Processo Telematico – 8.4. Comunicazioni telematiche. - 8.5. Considerazioni critiche.

Premessa.
L'attuazione del Decreto legislativo 07.09.2012 n° 155, G.U. 12.09.2012, meglio conosciuto come "revisione della Geografia Giudiziaria" ha comportato innovazioni anche a riguardo del processo telematico che, a mio avviso, sia per scarsa informativa sia per la tardività delle stesse, ha creato non pochi problemi e disagi "agli operatori del settore giustizia".

8.1 - Soppressione Uffici Giudiziari, SICID e Processo Telematico.

il 14 settembre 2013, in esecuzione del Decreto legislativo 07.09.2012 n° 155, G.U. 12.09.2012, sono stati soppressi 30 Tribunali e 220 sezioni con accorpamento degli Uffici Giudiziari soppressi a quelli rimanenti.
Prima di tale accorpamento le sedi centrali di Tribunale e le Sezioni distaccate catalogavano nel SICID (registro informatico per la cognizione civile) i vari fascicoli in registri informatici (SICID) separati: per cui era naturale avere il fascicolo 1/2013 della sede centrale del Tribunale e il fascicolo 1/2013 della relativa Sezione distaccata.
Premesso ciò mi chiedevo, in generale, come da settembre sarebbero stati gestiti, nel SICID della sede centrale del Tribunale, i dati dei Tribunali accorpati e quelli delle sezioni distaccate (ciò, soprattutto, per i depositi da effettuarsi tramite PCT per i procedimenti pendenti alla data del 14 settembre 2013 essendo impossibile la coesistenza, nel medesimo registro SICID, di fascicoli con la stessa numerazione) e, in particolare se DGSIA avesse comunicato agli Uffici Giudiziari come gestire tale problematica e come, conseguentemente, gli avvocati si sarebbero dovuti comportare per i depositi telematici.
La risposta al quesito arrivava da DGSIA, tutt'altro che tempestivamente, con la comunicazione apparsa il giorno 11 settembre 2013 sul Portale dei Servizi Telematici del Ministero della Giustizia[15] con la quale venivano definite le modalità di trattamento dei dati gestiti dai sistemi informatici in uso presso le cancellerie civili degli uffici giudiziari.
La comunicazione distingue due ipotesi diverse: la prima relativa alla soppressione delle Sezioni Distaccate di Tribunale e la seconda inerente la soppressione dei Tribunali Circondariali.

8.2 - Soppressione Sezioni Distaccate di Tribunale e Processo Telematico.

Sul punto DGSIA ha previsto che i procedimenti pendenti, alla data di soppressione dell'ufficio, venissero trasferiti presso la sede del tribunale di circondario ove avrebbero proseguito il loro iter nell'ufficio accorpante assumendo un nuovo numero di ruolo (prefisso numerico fisso associato alla sezione distaccata soppressa) risultando definiti "per trasferimento ad altra sede" nell'archivio informatico dell'ufficio soppresso.

[15] http://pst.giustizia.it/PST/resources/cms/documents/Accorpamento_UUGG_istruzioni_servizi_telematici_v52.pdf

L'iscrizione di un nuovo procedimento dal 14 settembre 2013, potrà essere effettuata unicamente presso l'ufficio accorpante (tribunale circondariale) con conseguente dismissione dell'indirizzo PEC della sezione distaccata.
In conseguenza di ciò aggiungeva che Il deposito telematico degli atti in corso di causa riguardanti procedimenti pendenti (alla data di soppressione della sezione distaccata) doveva eseguirsi esclusivamente utilizzando la casella di PEC dell'ufficio accorpante, avendo cura di individuare il procedimento attraverso il nuovo numero di ruolo assunto nell'ambito dell'ufficio accorpante.

8.3 - Soppressione dei Tribunali Circondariali e Processo Telematico.

DGSIA ha previsto che, da un punto di vista informatico, i procedimenti pendenti negli uffici soppressi rimanessero associati all'ufficio soppresso fino alla loro definizione, mantenendo inalterata la numerazione; agli operatori di cancelleria e ai magistrati il compito di gestire tali procedimenti accedendo (di volta in volta) ai registri di cancelleria dell'ufficio soppresso.
L'iscrizione di un nuovo procedimento dal 14 settembre 2013 potrà essere effettuata unicamente presso l'ufficio accorpante ma, in questa ipotesi e a differenza della prima, l'indirizzo PEC dell'ufficio giudiziario soppresso verrà mantenuto invariato per consentire il deposito telematico dei soli atti dei procedimenti in corso di causa.
Specificava altresì che Il deposito telematico degli atti in corso di causa riguardanti procedimenti pendenti (alla data di soppressione dell'ufficio giudiziario) doveva eseguirsi utilizzando comunque la casella PEC dell'ufficio soppresso mentre i depositi inerenti l'iscrizione a ruolo di nuovi procedimenti dovevano essere indirizzati alle caselle di PEC relative ad uffici non soppressi, secondo la competenza.
A decorrere dalla data di soppressione di un ufficio giudiziario, il valore legale relativo ai depositi telematici è conferito dal decreto ministeriale (ai sensi dell'art. 35 comma 1 del D.M. 44/2011) emesso per l'ufficio accorpante.

8.4 - Comunicazioni e notificazioni telematiche.

La comunicazione più sopra citata ha disposto anche in merito alle comunicazioni e notificazioni telematiche sia relativamente alle sezioni distaccate soppresse, sia per la soppressione dell'ufficio giudiziario.
Nel primo caso: le comunicazioni e le notificazioni relative ai procedimenti pendenti (alla data di soppressione della sezione distaccata) saranno inviate dall'indirizzo di PEC dell'ufficio accorpante mentre,
nel secondo caso: le comunicazioni e le notificazioni relative a procedimenti pendenti (alla data di soppressione dell'ufficio giudiziario) continueranno ad essere inviate dall'indirizzo di PEC associato all'ufficio soppresso. Il testo della comunicazione o della notificazione recherà la nuova denominazione associata all'ufficio soppresso.

8.5 - Considerazioni critiche.

In relazione a quanto sopra descritto, mi siano consentite alcune considerazioni critiche:
1) la comunicazione di DGSIA viene resa nota appena tre giorni prima dell'entrata in vigore e piena operatività del Decreto legislativo 07.09.2012 n° 155: è assurdo che decisioni così importanti vengano assunte e "comunicate" agli Uffici Giudiziari e all'avvocatura senza un doveroso e congruo anticipo.

2) la comunicazione di DGSIA viene resa nota con la pubblicazione della stessa sul Portale dei Servizi Telematici del Ministero della Giustizia: indubbiamente il detto Portale rappresenta il mezzo informativo ufficiale delle comunicazioni del Ministero della Giustizia aventi ad oggetto il processo telematico ma, considerando sia il ritardo con le quali le stesse sono state pubblicate (11 settembre 2013) rispetto all'entrata in vigore del D.Lgs. 155/2012 (14 settembre 2013) sia la delicatezza e importanza del contenuto delle informazioni, sarebbe stato opportuno che tale comunicazione DGSIA oltre che pubblicarle sul Portale di riferimento l'avesse inviata a Ciascun Consiglio dell'Ordine il quale avrebbe provveduto a sua volta a comunicarla, con ogni mezzo, ai propri iscritti molti dei quali, ad oggi, non ne hanno conoscenza proprio per tale difetto di comunicazione.
3) Nella prima ipotesi prevista dalla comunicazione, si fa riferimento ad un prefisso numerico fisso associato al numero di ruolo del procedimento esistente nella sezione distaccata soppressa.
Sul punto osservo che ad oggi (fine ottobre 2013) NON ESISTE ELENCO UFFICIALE dal quale poter evincere quali siano i prefissi numerici scelti dagli Uffici Giudiziari ed abbinati al numero di ruolo del procedimento esistente nella sezione distaccata soppressa!
Qualcuno potrebbe dire, a tal proposito, che gli uffici giudiziari accorpanti, inserendo nel SICID il procedimento acquisito dalla sede distaccata accorpata, inoltrano automaticamente all'avvocato un biglietto di cancelleria tramite PEC nel quale si evince (per la verità in maniera poco chiara in quanto nessun riferimento viene fatto al motivo per cui la PEC viene inoltrata) il nuovo numero di ruolo contenente il famigerato prefisso numerico così come comunicato da DGSIA, in maniera altrettanto INTEMPESTIVA, il giorno 23 settembre 2013[16]; a tale "eccezione" rispondo affermando che sono moltissimi i procedimenti "dimenticati" nelle Sezioni Distaccate soppresse, non trasferiti al SICID dell'Ufficio Giudiziario accorpante e per i quali, quindi, non è stato inoltrato nessun biglietto di cancelleria tramite PEC con la conseguenza che, da una parte il professionista rimane assolutamente ignaro circa il prefisso numerico aggiunto all'esistente numero di ruolo e, dall'altra, causa la mancanza del "trasferimento informatico" dal SICID della Sezione Distaccata soppressa a quello del Tribunale accorpante E' IMPOSSIBILITATO A DEPOSITARE TELEMATICAMENTE ATTI E/O DOCUMENTI!
Quanto ai procedimenti "dimenticati" posso affermare, per esperienza personale, che la maggior parte è relativa a procedimenti processualmente interrotti o a procedimenti assunti in decisione ma per i quali ancora non sono decorsi i termini per il deposito di comparse conclusionali e/o repliche.
In questi casi all'avvocato altro non rimane da fare che recarsi personalmente in cancelleria e segnalare la disfunzione; le cose naturalmente si complicano ove il professionista riscontri un tale disservizio in un Tribunale diverso da quello in cui opera prevalentemente.
A conferma delle problematiche e dei disagi derivanti da tale "soluzione" segnalo il decreto n. 108[17] a firma del Dott. Michele Galluccio, Presidente del Tribunale di Barcellona Pozzo di Gotto il quale, il 17 ottobre 2013, invita **"…i Sigg. Avvocati a non procedere, sino a nuova disposizione, al deposito telematico degli atti relativi a procedimenti già di competenza delle soppresse Sezioni distaccate di Lipari e Milazzo…"**.

[16] http://pst.giustizia.it/PST/it/pst_3_1.wp?previousPage=pst_3&contentId=NEW806

[17] http://www.ordineavvocatibarcellonapg.it/UserFiles//File/decreti_Tribunale/Decreto_del_Presidente_del_Tribunale_di_Barcellona_P.G._n._108_del_17.10.2013.pdf

CAPITOLO IX
Il Processo Penale Telematico

Sommario: Premessa - 9.1. Il Servizio Procura ex 335 c.p.p. – 9.2. Il Servizio Procura 415 bis c.p.p. – 9.3. Il Servizio Trascrizioni Verbali di Udienza.

Premessa.
Il processo telematico e l'utilizzo della telematica in generale ha visto, come principale protagonista, il professionista impegnato nella trattazione di procedimenti civili "trascurando", quindi, gli avvocati che, esclusivamente o prevalentemente, operavano nel settore penale.
Pur non essendo possibile parlare di un vero e proprio processo penale telematico, ritengo però giusto ed opportuno aprire, per chi opera in tale settore, una piccola finestra attraverso la quale, anche l'avvocato penalista, potrà fruire dei benefici telematici nello svolgimento della sua attività professionale.
Sono già operativi infatti alcuni servizi penali, riconosciuti sotto il profilo legale dal Ministero della Giustizia, che consentono al penalista di svolgere adempimenti senza doversi recare personalmente nell'ufficio giudiziario.
Ad oggi i servizi attivi in diversi uffici giudiziari sono i seguenti:

- Servizio Procura ex 335 c.p.p.

- Servizio Procura 415 bis c.p.p

- Servizio Trascrizione Verbali di Udienza

9.1. – Il Servizio Procura ex 335 c.p.p.

Consente all'avvocato munito di mandato difensivo della persona indagata e/o parte offesa di un procedimento penale di richiedere e ricevere le informazioni di cui all'art.335 c.p.p. accedendo in via informatica alla Segreteria dedicata della Procura, ove tale servizio è attivo, senza necessità di recarsi presso il relativo sportello.
La fase delle indagini preliminari (nella quale si esercita gran parte dell'attività delle Procure della Repubblica) è coperta dal segreto istruttorio e ciò, non solo per ovvi motivi legati essenzialmente al buon esito delle indagini in corso, ma anche per esigenze di tutela della riservatezza delle persone eventualmente coinvolte.
Il registro delle notizie di reato (tenuto dalle Procure), nel quale vengono iscritti i nominativi delle persone indagate e/o delle persone offese, è, quindi, un registro riservato. Il suo contenuto può infatti essere comunicato solo a determinati soggetti e secondo le prescrizioni della legge.
Il legislatore, anche per porre rimedio ad ingiustificate fughe di notizie, con la legge n. 332 del 1995 ha previsto che l'indagato e/o la persona offesa (ed il loro difensore) possano conoscere se il proprio nominativo è presente nel registro delle notizie di reato. L'Ufficio, salvo che il magistrato vieti la comunicazione, comunica le risultanze del registro, cioè:
1) nulla, se non vi è alcuna iscrizione (ovvero se il magistrato ha vietato la comunicazione);
2) il numero del procedimento, il reato ed il nome del magistrato titolare dell'indagine, in caso di iscrizioni positive.

Il certificato ex art. 335 c.p.p. attesta, quindi, l'esistenza o meno di iscrizioni nel registro delle notizie di reato.
Tale servizio, nella sua fruibilità telematica, comporta notevoli vantaggi quali:
- la maggiore celerità con la quale avverrà il rilascio delle attestazioni ex art.335 c.p.p.;
- il risparmio di risorse di cui fruirà l'avvocatura esonerata dalla necessità di accedere fisicamente agli sportelli della Procura;
- l'incremento in termini di efficienza del servizio pubblico assicurato dall'amministrazione giudiziaria che, d'altro canto, vedrà meglio tutelate anche le ragioni di sicurezza grazie al ridursi del numero delle persone che quotidianamente affluiranno nel palazzo di giustizia.
Il servizio è attualmente in uso presso i seguenti Uffici Giudiziari:
Bari[18], Brindisi, Campobasso, Catania, Chiavari, Firenze, Foggia, Forlì, Cesena, Gela, Genova[19], Isernia, Larino, La Spezia, Matera, Napoli[20], Oristano, Palermo, Rimini, Roma[21], Sala Consilina, Santa Maria Capua Vetere,, Savona, Siracusa, Taranto, Termini Imerese, Trapani, Venezia[22], Vercelli

9.2. – Il Servizio Procura 415 bis c.p.p.

Il **Servizio Procura 415 bis** consente di richiedere e ottenere telematicamente copia dei verbali delle indagini preliminari, permettendo il pagamento telematico dei diritti di copia in tempo reale.
Tale servizio quindi eviterà all'avvocato di accedere fisicamente alla cancelleria evitando quindi che il difensore effettui il primo accesso per visionare il fascicolo e per depositare materialmente la richiesta di copie e il secondo per il ritiro delle copie richieste.
Ciò vuol dire per il difensore la possibilità di risparmiare tempo per la conoscenza del contenuto del fascicolo ed essere quindi avvantaggiato per predisporre quanto opportuno per la difesa del proprio assistito considerando soprattutto che dalla ricezione dell'avviso ex art. 415 bis c.p.p. lo stesso ha solo venti giorni per presentare memorie, produrre documenti, depositare le investigazioni difensive, chiedere al PM atti di indagine, far presentare l'assistito per rilasciare dichiarazioni o, infine, chiedere che il proprio assistito venga sottoposto ad interrogatorio.
Il servizio è attualmente in uso presso l'Ufficio Giudiziario di Matera[23].

9.3. – Il Servizio Trascrizione Verbali di Udienza

E' il servizio che consente di richiedere la copia digitale delle trascrizioni delle udienze penali consentendo inoltre il pagamento telematico dei diritti di copia.
Il servizio consente di recuperare la copia digitale delle trascrizioni delle udienze penali di tutti i processi presso gli Uffici Giudiziari italiani in cui il servizio è attivo.
L'avvocato potrà pertanto dal proprio studio e, comunque, da qualsiasi luogo dal quale risulta possibile connettersi ad internet, accedere alla banca dati ministeriale delle trascrizioni, pagare on line gli eventuali diritti di cancelleria dovuti ed estrarre copia informatica della trascrizione di cui ha necessità.

---

[18] http://www.ordineavvocati.bari.it/default.asp?idlingua=1&rif=23&guid=54
[19] http://www.ordineavvocatigenova.it/node/8872
[20] http://www.ordineavvocati.napoli.it/public/AllegatiNews/20120508103635l6proc335.pdf
[21] http://www.ordineavvocatiroma.it/documenti/16573.pdf
[22] http://www.ordineavvocativenezia.net/CMS/processo-penale-telematico/257-richiesta-e-rilascio-delle-informative-ex-art-335-cpp-per-via-telematica
[23] http://www.ordineavvocatimatera.it/Documenti/lettera_DGSIA.pdf

Il sistema utilizza una particolare funzione che calcola automaticamente il numero delle pagine della trascrizione d'udienza di cui si chiede la copia e di conseguenza l'importo dei diritti di cancelleria dovuti per legge che saranno pagati sempre online.
Le copie digitali delle trascrizioni saranno disponibili e scaricabili per l'avvocato soltanto successivamente al buon fine della procedura per il pagamento dei diritti di cancelleria.
Il rilascio è assolutamente automatizzato e non è necessario alcun intervento da parte del personale di cancelleria per concludere il procedimento per il recupero della copia delle trascrizioni. Al personale è devoluta una semplice attività di controllo formale sul corretto rilascio delle copie.
L'accesso al sistema avviene esclusivamente tramite dispositivo di autenticazione digitale (firma digitale) affinché sia certa l'identità del soggetto richiedente.
Il servizio è in uso sperimentale presso gli Uffici Giudiziari di:
Palermo, Roma, Bari, La Spezia[24].

[24] http://www.ordineavvocatidellaspezia.it/visualizzazioni/vedi_dettagli.php?areanumber=21&idmessaggio=384

CAPITOLO X
Il Processo Tributario Telematico

Sommario: Premessa - 10.1. Le attività telematiche nel processo tributario – 10.2. L'utilizzo della PEC nel processo tributario.

Premessa.
Il 23 dicembre 2009 veniva siglato il protocollo di intesa[25] tra il Dipartimento delle Finanze del Ministero dell'Economia e delle Finanze, il Consiglio di Presidenza della Giustizia Tributaria, l'Agenzia delle Entrate e il Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili che avviava formalmente la sperimentazione del Processo Tributario telematico e, nel febbraio 2010 la sperimentazione iniziava presso la Commissione tributaria provinciale e quella regionale del Lazio; il 1 giugno 2010 il citato protocollo d'intesa veniva esteso anche al Consiglio Nazionale Forense.
Il 25 luglio 2013, il Consiglio di Stato ha dato parere favorevole, con alcuni rilievi, allo schema di regolamento recante la disciplina sull'uso di strumenti informativi e telematici nell'ambito del processo tributario (Parere Consiglio di Stato 25/07/2013, n. 3451) [26]; parere favorevole era stato già rilasciato il giorno 08 novembre 2012 dal Garante per la protezione dei dati personali al MEF[27] ed è attesa, entro il 2013, la sua pubblicazione in Gazzetta Ufficiale.

10.1. – Le attività telematiche nel processo tributario
La sperimentazione dell'applicazione informatica, che permette l'interazione telematica delle procedure del contenzioso tributario, si basa sull'uso della posta elettronica certificata (PEC) e della firma digitale e, consentirà, tra l'altro:
- il deposito telematico presso le Commissioni tributarie dei ricorsi e degli altri atti processuali;
- la comunicazione del dispositivo delle sentenze alle parti;
- l'accesso telematico delle parti al fascicolo informatico del processo.

Il Processo Tributario telematico ridurrà in modo significativo tempi e costi del contenzioso, nel rispetto dei criteri di efficienza, efficacia, economicità e trasparenza dell'azione amministrativa.
Attualmente l'accesso al **Sistema Informativo della Giustizia Tributaria (S.I.GI.T.) è consentito esclusivamente agli utenti autorizzati che hanno aderito al progetto di sperimentazione**.
Il regolamento si applicherà a tutti gli atti e provvedimenti del processo tributario, compresi quelli relativi al procedimento attivato con il reclamo e la mediazione il quale è obbligatorio per impugnare le contestazioni del Fisco emesse dalle Entrate per un valore fino a 20mila euro. In pratica, i documenti saranno firmati digitalmente e "viaggeranno" tramite S.i.g.i.t. (Sistema informativo della giustizia tributaria). Chi ha utilizzato in primo grado le modalità telematiche sarà

[25] http://www.agenziaentrate.gov.it/wps/file/nsilib/nsi/agenzia/agenzia+comunica/comunicati+stampa/archivio+comunicati/cs+2010/cs+gennaio+2010/cs+130110+processo+tributario+telematico/PROCESSO+TRIBUTARIO+TELEMATICO.pdf

[26] http://fiscopiu.it/sites/default/files/Consiglio%20di%20Stato%20Parere%2025%20luglio%202013%20n.%203451.pdf

[27] http://www.privacy.it/garanteprovv201211082.html

tenuto a impiegare sempre le stesse per tutto il percorso giudiziale e anche in appello. Unica eccezione è rappresentata dalla sostituzione del difensore[28].

10.2. – L'utilizzo della PEC nel processo tributario

Dal 15 maggio 2012, a seguito del decreto 26 aprile 2012, n. 7425 pubblicato sulla Gazzetta Ufficiale n. 102 del 3 maggio 2012, anche nel processo tributario è stata introdotta la PEC per le le notificazioni e le comunicazioni di cui all'articolo 16, comma I-bis, del decreto legislativo 31 dicembre 1992, n. 546, da inviare da parte degli Uffici di segreteria delle CTP e CTR relativamente ai ricorsi notificati a decorrere dal 7 luglio 2011 anche se ciò, inizialmente, limitatamente in due sole Regioni (Friuli e Umbria) per poi estendersi a tutte le Commissioni Tributarie a seguito della emanazione del regolamento attuativo sul processo telematico[29] che, dovrebbe vedere la sua pubblicazione in Gazzetta Ufficiale entro il 2013.

[28] http://iusletter.com/il-processo-tributario-fara-il-pieno-di-atti-online/

[29] http://www.altalex.com/index.php?idnot=18130

CAPITOLO XI
Processo Telematico e procedure concorsuali

Sommario: Premessa - 11.1. Come cambia la procedura fallimentare – 11.2. Come cambia la procedura di concordato preventivo – 11.3. Come cambia la procedura di amministrazione straordinaria – 11.4. Come cambia la procedura di liquidazione coatta amministrativa.

Premessa.

Con l'entrata in vigore della Legge 17 dicembre 2012 n. 221, di conversione del D.L. 18 ottobre 2012 n. 179 successivamente integrata dalla Legge 24 dicembre 2012 n. 228 (Legge di Stabilità 2013), sono state introdotte significative modifiche alla disciplina delle comunicazioni degli atti nelle procedure concorsuali ponendo nuovi immediati adempimenti a carico dei curatori, dei commissari giudiziali e dei liquidatori nei concordati preventivi nonché dei commissari delle amministrazioni straordinarie e delle liquidazioni coatte amministrative, anche con riguardo a procedure concorsuali già pendenti a quella data.

Le nuove disposizioni si sono applicate, quindi, dal 19 dicembre 2012 non solo a tutte le nuove procedure di fallimento, concordato preventivo, liquidazione coatta amministrativa ed amministrazione straordinaria attivate dopo il 19 dicembre 2012 ma anche a quelle già pendenti a tale data a condizione che non fosse stata ancora inviata ai creditori, alla data del 19 dicembre 2012, l'avviso previsto dagli articoli 92, 171, 207 Legge Fallimentare e dall'art. 22 D.Lgs. n. 270/99.

Per tutte le procedure sopra richiamate e per le quali, alla data del 19 dicembre 2012, il citato avviso sia stato già effettuato, le nuove disposizioni si applicano a decorrere dal 31 ottobre 2013.

Il Tribunale di Milano, con la comunicazione di servizio n. 40/2012[30], ha predisposto indicazioni operative per l'applicazione della nuova disciplina.

11.1. - Come cambia la procedura fallimentare.

La nuova normativa prevede che:

1) entro 10 giorni dalla nomina, il curatore fallimentare deve comunicare al Registro delle Imprese, ai fini dell'iscrizione, il proprio indirizzo di posta elettronica certificata (P.E.C.);

2) il curatore deve inviare l'avviso ex art. 92 Legge Fallimentare all'indirizzo PEC dei creditori o dei titolari di diritti sui beni risultante dal Registro delle Imprese e/o dall'Indice Nazionale degli indirizzi di Posta elettronica Certificata delle Imprese e dei Professionisti, mentre deve continuare ad inviarlo tramite raccomandata o fax presso la sede dell'impresa o la residenza del creditore a coloro i quali siano sforniti di tale indirizzo PEC o il cui indirizzo PEC non risulti reperibile nel Registro delle Imprese o nell'Indice Nazionale degli indirizzi di Posta elettronica Certificata delle Imprese e dei Professionisti;

3) in ogni caso il Curatore, con l'avviso ex art. 92 Legge Fallimentare, deve comunicare ai destinatari il proprio indirizzo PEC, avvisandoli:

a) che le domande di ammissione al passivo o di rivendica o restituzione dei beni possono essere presentate, unitamente ai relativi documenti, unicamente mediante trasmissione a tale indirizzo (PEC);

b) che nella domanda il ricorrente deve indicare l'indirizzo PEC al quale intende ricevere le successive comunicazioni;

[30] https://www.tribunale.milano.it/files/fallimenti/Circolari/comunicazione_27122012.pdf

c) che, in caso di omessa indicazione dell'indirizzo PEC, tutte le comunicazioni verranno effettuate esclusivamente mediante deposito in cancelleria;
4) la spedizione delle domande (tempestive o tardive) all'indirizzo PEC del curatore, sia digitalmente sottoscritte, sia con sottoscrizione apposta sull'originale del documento (cartaceo) successivamente oggetto di scansione digitale, deve essere effettuata da un indirizzo PEC, anche non di appartenenza del ricorrente (ad es. un professionista, o un'associazione sindacale o di categoria);
5) gli unici documenti che il ricorrente deve e può depositare in cancelleria in originale cartaceo sono i titoli di credito;
6) il curatore, almeno 15 giorni prima dell'udienza di verifica, deve trasmettere il progetto di stato passivo e le domande alla cancelleria e deve contestualmente comunicare il progetto di stato passivo agli indirizzi PEC indicati dai ricorrenti;
7) le eventuali osservazioni al progetto di stato passivo possono essere presentate, entro il termine di cinque giorni prima dell'udienza di verifica, esclusivamente mediante il loro invio all'indirizzo PEC del curatore;
8) in ossequio alla regola generale introdotta con il nuovo art. 31-bis Legge Fallimentare, tutte le successive comunicazioni che la legge o il Giudice pone a carico del curatore sono da quest'ultimo effettuate agli indirizzi PEC indicati dai creditori e dai titolari di diritti sui beni, mentre, nel caso di omessa indicazione o di impossibilità di consegna del messaggio di posta elettronica certificata per cause imputabili al destinatario, le comunicazioni verranno fatte esclusivamente mediante deposito in cancelleria;
9) la PEC dovrà essere utilizzata, oltre che per la comunicazione del progetto di stato passivo, anche per la comunicazione dei seguenti e ulteriori atti: lo stato passivo; le relazioni semestrali ex art. 33 Legge Fallimentare, i progetti di riparto parziali, il rendiconto, il progetto di riparto finale, la proposta di concordato fallimentare (ed i relativi pareri), il decreto con cui il Tribunale, ai sensi dell'art. 102 Legge Fallimentare, dispone di non farsi luogo all'accertamento del passivo e, da ultimo, il ricorso per esdebitazione;
10) è fatto obbligo al curatore di conservare tutti i messaggi inviati e ricevuti a mezzo PEC sia in pendenza di procedura sia fino a due anni successivi alla chiusura del fallimento.

Come già anticipato, per i fallimenti nei quali l'avviso ex art. 92 Legge Fallimentare risulti essere già inviato alla data del 19 dicembre 2012, la nuova disciplina si è applicata a partire dal 31 ottobre 2013 e il curatore, in queste procedure, avrà assolto l'obbligo di comunicare a tutti i creditori ammessi e ai titolari di diritti su beni, entro il 30 giugno 2013, il suo indirizzo PEC, richiedendo ai destinatari di comunicare il proprio entro tre mesi.

11.2. - Come cambia la procedura di concordato preventivo.

La nuova normativa prevede che:
a) il Commissario Giudiziale entro dieci giorni dalla nomina deve comunicare al Registro delle Imprese, ai fini dell'iscrizione, il proprio indirizzo di posta elettronica certificata e, dopo la nomina deve comunicare all'indirizzo PEC dei creditori, se risultante dal Registro delle Imprese e/o dall'Indice Nazionale degli indirizzi di Posta elettronica Certificata delle Imprese e dei Professionisti, o altrimenti raccomandata o fax, l'avviso contenente il suo indirizzo PEC, la data stabilita per la convocazione dei creditori, la proposta di concordato, il decreto di ammissione, l'invito ai creditori di comunicare entro giorni quindici gli indirizzi PEC ai quali intendono ricevere le successive comunicazioni con l'avvertimento che, nell'ipotesi di omessa indicazione, le stesse saranno effettuate esclusivamente mediante deposito in cancelleria;

b) tutte le successive comunicazioni del Commissario Giudiziale ai creditori sono effettuate all'indirizzo PEC da essi indicato e, in caso di mancata indicazione o di impossibilità di consegna del messaggio con tale modalità per cause imputabili al destinatario, le stesse verranno fatte esclusivamente mediante deposito in cancelleria;
c) è fatto obbligo al Commissario Giudiziale di conservare tutti i messaggi inviati e ricevuti a mezzo PEC sia in pendenza di procedura sia fino a due anni successivi alla chiusura della stessa;
d) tra gli atti che il Commissario Giudiziale deve comunicare all'indirizzo PEC dei creditori sono espressamente previsti la relazione ex art. 172 Legge Fallimentare, per la quale adesso è fissato il termine di giorni dieci prima dell'adunanza, e il decreto di apertura del procedimento di revoca del concordato ex art. 173 Legge Fallimentare;
e) nell'ipotesi di omologa di concordato preventivo che preveda la cessione dei beni ai creditori, il liquidatore giudiziale deve, semestralmente, redigere un rapporto sull'andamento della liquidazione, inviandone copia al comitato dei creditori, unitamente alla documentazione bancaria, per le eventuali osservazioni, ed una copia al Commissario Giudiziale che, a sua volta, provvede a comunicarla a tutti i creditori ai rispettivi indirizzi PEC o, se non indicati, mediante deposito in cancelleria.

La nuova disciplina si è applicata ai nuovi concordati preventivi introdotti a partire dal 19 dicembre 2012 nonché a quelli già aperti nei quali non fosse stata ancora effettuata, alla data del 19 dicembre 2012, la comunicazione della data di adunanza.
Per i concordati già aperti al 19 dicembre 2012 la nuova disciplina si applica invece a partire dal 31 ottobre 2013. In queste procedure il Commissario Giudiziale avrà dovuto comunicare a tutti i creditori, entro il 30 giugno 2013, il suo indirizzo PEC, richiedendo ai destinatari di comunicare il proprio entro tre mesi.

11.3. - Come cambia la procedura di amministrazione straordinaria.
La nuova normativa prevede che:
a) il Commissario entro dieci giorni dalla nomina deve comunicare al Registro delle Imprese, ai fini dell'iscrizione, il proprio indirizzo di posta elettronica certificata e deve altresì comunicare tale indirizzo PEC ai creditori ed ai terzi titolari di diritti sui beni ai relativi indirizzi PEC se risultanti dal Registro delle Imprese e/o dall'Indice Nazionale degli indirizzi di Posta elettronica Certificata delle Imprese e dei Professionisti, o altrimenti a mezzo raccomandata o fax;
b) tra gli atti che il Commissario deve comunicare agli indirizzi PEC dei creditori ed ai terzi titolari di diritti sui beni, o mediante deposito in cancelleria in caso di mancata indicazione degli stessi, la legge espressamente prevede: la relazione del commissario sulle cause dello stato d'insolvenza e sulla sussistenza delle condizioni ai fini dell'ammissione dell'impresa alla procedura di amministrazione straordinaria , il programma autorizzato, le relazioni trimestrali sull'esecuzione del programma, la relazione finale e il bilancio finale con il conto della gestione.

La nuova disciplina si è applicata alle nuove procedure di amministrazione straordinaria introdotte dopo il 19 dicembre 2012 nonché a quelle già aperte nelle quali non fosse stato ancora effettuato, alla data del 19 dicembre 2012, l'invio ai creditori dell'avviso per l'accertamento del passivo di cui all'art. 22 D.Lgs. 270/1999.
Per le procedure già aperte e nelle quali l'avviso invece sia stato inviato prima del 19 dicembre 2012, la nuova disciplina si applica invece a partire dal 31 ottobre 2013. In queste procedure il Commissario avrà dovuto comunicare a tutti i creditori, entro il 30 giugno 2013, il suo indirizzo PEC, richiedendo ai destinatari di comunicare il proprio entro tre mesi.
11.4. - Come cambia la procedura di liquidazione coatta amministrativa.

La nuova normativa prevede che:
fatte salve alcune deroghe previste per le forme soggette a rito speciale valgono, per tale procedura, regole analoghe a quelle dettae per le amministrazioni straordinarie, salvo le varianti dovute al diverso iter di formazione del progetto di stato passivo.

CAPITOLO XII
Il pagamento telematico delle spese di giustizia

Sommario: Premessa - 12.1. Pagamenti telematici delle spese di giustizia: applicazione e utilizzazione.

Premessa.
E' possibile eseguire in modalità telematica anche i pagamenti relativi a spese di giustizia, diritti e contributo unificato così come previsto dalla normativa vigente, dal Codice dell'Amministrazione Digitale (D. Lgs 235/2010 art. 5) e dal D.M. 44 del 12 febbraio 2011.

12.1 - Pagamenti telematici: applicazione e utilizzazione.

I pagamenti telematici si applicano agli ambiti processuali civile e penale, per servizi presso tutti gli uffici giudiziari: tribunali, procure, giudici di pace, cassazione e sono attivabili indipendentemente dal livello di informatizzazione degli uffici giudiziari.

I pagamenti telematici possono essere utilizzati per pagamento del contributo unificato e dei diritti di cancelleria mentre, per il pagamento dei diritti di copia, lo stesso è previsto in via sperimentale presso i seguenti otto tribunali:
Milano, Genova, Bologna, Napoli, Padova, Modena, Verona e Rimini[31].
L'attestazione dell'avvenuto pagamento è un documento informatico rilasciato dal soggetto autorizzato ad erogare servizi di pagamento e da questi firmato digitalmente. Il documento informatico ha valore "liberatorio" per il soggetto a nome del quale è stato eseguito il pagamento.
Il pagamento su canale telematico dei diritti e delle spese di giustizia è eseguito secondo le regole tecniche di cui al DM 44/2011 e le relative specifiche tecniche definite nel provvedimento del 18 luglio 2011.
Tale servizio permette, quindi, all'avvocato di pagare on-line le spese di giustizia ed i diritti. Il pagamento telematico può essere eseguito attraverso i canali indicati dal Punto di Accesso privato o dal Portale dei servizi Telematici del Ministero della Giustizia.
Le informazioni necessarie per poter procedere al pagamento telematico sono:

- l'indicazione dell'ufficio giudiziario;

- la causale del pagamento: contributo unificato, diritti di cancelleria, diritto di copia; sul punto preciso che Il contributo unificato e i diritti di cancelleria necessari per l'iscrizione a ruolo possono essere versati con una unica operazione;

- l'importo da versare;

[31] http://www.giustiziacampania.it/opencms/export/sites/default/giustiziacampana/napoli_cisia/menu/Documenti/pagamenti_telematici.pdf

- l'indicazione del soggetto pagatore (colui che esegue materialmente in versamento - titolare dello strumento di pagamento);
- l'indicazione del soggetto versante (soggetto debitore nei confronti della pubblica amministrazione).

A fronte di una operazione di pagamento, il sistema restituisce una ricevuta di avvenuto versamento (ricevuta telematica, indicata con l'acronimo RT), nella forma di documento informatico firmato digitalmente dal soggetto scelto come erogatore del servizio di pagamento (prestatore di servizio di pagamento), e contenente, tra le altre, le seguenti informazioni:

- l'identificativo univoco di pagamento – permette di individuare un pagamento, nei confronti del Ministero della Giustizia, in maniera univoca e certa;

- l'esito del pagamento. Nel caso in cui con una unica operazione sia stato eseguito il versamento per contributo unificato e diritti di cancelleria, sarà dettagliato anche l'esito di ogni singolo pagamento;

- la causale di ogni singolo versamento;

- l'istituto attestante l'avvenuto pagamento.

La ricevuta così ottenuta può essere utilizzata sia nell'ambito di un flusso telematico **"salvando" sul computer la ricevuta elettronica e allegandola nella busta telematica creata per il deposito telematico** (a norma del DM 44/2011) sia in modalità tradizionale, consegnando all'ufficio giudiziario la stampa della ricevuta come attestazione dell'avvenuto pagamento.

Ad oggi i pagamenti telematici delle spese di giustizia sono attivi nei seguenti 105 Uffici Giudiziari:

Corti d'Appello (20):
Ancona, Bari, Bologna, Campobasso, Catania, Catanzaro, Firenze, Genova, L'Aquila, Lecce, Messina, Napoli, Palermo, Perugia, Potenza, Reggio Calabria, Roma, Taranto, Torino, Venezia

Tribunali (85):
Acqui Terme, Alba, Alessandria, Ancona (tutti gli uffici del Distretto), Aosta, Arezzo, Ascoli Piceno, Asti, Avezzano, Bari, Biella, Bologna (tutti gli uffici del Distretto), Caltagirone, Camerino, Casale Monferrato, Campobasso, Catania (tutti gli uffici del Distretto), Catanzaro, Chieti, Cuneo, Fermo, Ferrara, Firenze (tutti gli uffici del Distretto), Forlì, Genova (tutti gli uffici del Distretto), Grosseto, Ivrea, Lanciano, L'Aquila, Lecce (tutti gli uffici del Distretto), Livorno, Lucca, Lucera, Macerata, Milano (tutti gli uffici del Distretto) Messina (tutti gli uffici del Distretto), Modena, Modica, Mondovì, Montepulciano, Napoli (tutti gli uffici del Distretto), Novara, Palermo, Parma, Perugia, Pesaro, Pescara, Piacenza, Pinerolo, Pisa, Pistoia, Potenza, Prato, Ragusa, Ravenna, Reggio Calabria, Reggio Emilia, Rimini, Roma, Saluzzo, Siena, Siracusa, Sulmona, Taranto, Teramo, Torino, Tortona, Urbino, Vasto, Venezia, Verbania, Vercelli

CAPITOLO XIII
Le notifiche telematiche degli avvocati tramite PEC

Sommario: Premessa - 13.1. Le modifiche apportate alla L. 53/94 dalla L. 24.12.12 n. 228 e dal DM 48/2013 – 13.2. Il procedimento da seguire per la notifica tramite PEC – 13.3. Notifica tramite PEC ex L. 53/94 e (impossibile) deposito telematico dell'atto notificato presso l'Ufficio Giudiziario. – 13.4. Notifiche avvocati tramite PEC: dubbi circa l'effettiva possibilità del loro utilizzo prima del 15 dicembre 2013.

Premessa.
La legge 21 gennaio 1994 n. 53 ha conferito agli avvocati la possibilità di effettuare notifiche in proprio e, tale normativa è stata integrata con l'entrata in vigore della legge 148/2011 prevedendo quest'ultima che gli avvocati potessero effettuare tali notifiche anche utilizzando la posta elettronica certificata.
Vediamo come la normativa è ancor di più cambiata a seguito sia dell'entrata in vigore della legge 24 dicembre 2012 n. 228 sia della pubblicazione del decreto ministeriale 48/2013.

13.1 - Le modifiche apportate alla L. 53/94 dalla L. 24.12.12 n. 228 e dal DM 48/2013.

Le modifiche più importanti introdotte con la legge 24 dicembre 2012 n. 228 (che con l'art. 1 comma 19 apportava modifiche al DL 18.10.12 n. 179 modificando l'art. 16 e introducendo gli artt. 16 bis, ter e quater) venivano dalla stessa subordinate alla pubblicazione, nella Gazzetta Ufficiale, del decreto previsto dal numero 2 dell'art. 16 quater che avrebbe apportato modifiche all'art. 18 delle regole tecniche previste dal DM 44/2011.
Il 3 aprile 2013 veniva emanato il DM n. 48, pubblicato nella Gazzetta Ufficiale n. 107 del 09 maggio 2013 recante le modifiche all'art. 18 delle regole tecniche del DM 44/2011 per cui **il 24 maggio 2013 sono divenute operative le modifiche introdotte dalla legge 24 dicembre 2012 n. 228.**
Passerò in rassegna le modiche apportate dal DM 3.4.13 n. 48 collegandole con la legge 21 gennaio 1994 n. 53 per descrivere come gli avvocati dal 24 maggio 2013 possono effettuare notifiche in proprio a valore legale avvalendosi, quale strumento di notifica, della posta elettronica certificata.

Le novità più importanti sono le seguenti:
1) il titolo del nuovo art. 18 del DM 44/2011 "Notificazioni per via telematica eseguite dagli avvocati" che sostituisce il precedente "Notificazione per via telematica tra avvocati" e,
2) il richiamo esplicito, al comma 1 del nuovo art. 18, all'art. 3 bis della legge 21 gennaio 1994 n. 53.
Tali modifiche meritano rilievo in quanto si evince che la PEC, come mezzo per le notifiche degli avvocati, potrà essere utilizzata non solo quando destinatario della notifica sia altro avvocato ma anche quando destinatario sia persona diversa dall'avvocato a condizione, naturalmente, che l'indirizzo PEC del destinatario risulti da pubblici elenchi (art. 3 bis n. 1 legge 21 gennaio 1994 n. 53.).

L'Avvocato è considerato pubblico ufficiale.
L'art. 18 nuova formulazione con il comma 4 conferma e ribadisce quanto già indicato all'art. 6 della L. 53/94 e quindi che l'avvocato è considerato pubblico ufficiale ad ogni effetto di legge

quando compila la relazione o le attestazioni di cui agli artt. 3, 3 bis e 9 della legge 21 gennaio 1994 n. 53.
L'avvocato quindi potrà procedere alla notifica non solo di atti di sua produzione ma anche di quelli prodotti da soggetti diversi; in questo secondo caso estrae copia informatica per immagine dell'atto formato su supporto analogico (cartaceo), compie l'asseverazione prevista dall'art. 22 comma 2 del codice dell'amministrazione digitale, avendo cura di inserire la dichiarazione di conformità all'originale (cartaceo) nella relazione di notificazione così come previsto dall'art. 3 bis comma 5 della legge 21 gennaio 1994 n. 53.

La procura alle liti.
L'art. 18 del DM 44/2011 ora prevede altresì, al comma 5, che la **procura alle liti** si considera apposta in calce all'atto cui si riferisce quando è rilasciata su documento informatico separato allegato al messaggio di posta elettronica certificata mediante il quale l'atto è notificato. Tale disposizione inoltre si applica anche quando la procura alle liti è rilasciata su foglio separato del quale è estratta copia informatica, anche per immagine. Ciò significa che l'avvocato potrà, ad esempio, notificare ad un soggetto il cui indirizzo PEC risulti da pubblici elenchi l'atto di citazione avendo cura di allegare al messaggio PEC da inviare ai fini della notifica sia l'atto di citazione sia la procura alle liti rilasciata dal cliente.

Ricevuta PEC avvenuta consegna.
Il comma 6 dell'art. 18 del DM 44/2011 dispone ora che la ricevuta di avvenuta consegna del messaggio PEC con il quale l'atto viene notificato dovrà essere quella COMPLETA.

13.2 - Il procedimento da seguire per la notifica tramite PEC.

Vediamo ora cosa materialmente e nel concreto dovrà fare l'avvocato affinché possa eseguire la notifica a mezzo PEC senza, si spera, correre il rischio di andare incontro ad eventuali eccezioni.
1) essere in possesso di casella PEC comunicata all'Ordine di appartenenza e di firma digitale.
2) fare richiesta al proprio Consiglio dell'Ordine al fine di ottenere l'autorizzazione per effettuare le notifiche ai sensi della legge 21 gennaio 1994 n. 53; tale autorizzazione potrà essere concessa esclusivamente agli avvocati che non abbiano procedimenti disciplinari pendenti e che non abbiano riportato la sanzione disciplinare della sospensione dall'esercizio professionale o altra più grave sanzione e dovrà essere prontamente revocata in caso di irrogazione delle dette sanzioni ovvero, anche indipendentemente dall'applicazione di sanzioni disciplinari, in tutti i casi in cui il Consiglio dell'Ordine, anche in via cautelare, ritenga motivatamente inopportuna la prosecuzione dell'esercizio delle facoltà previste dalla legge 21 gennaio 1994 n. 53 (art. 7 L. 21 gennaio 1994 n. 53).
Solo dopo la delibera di autorizzazione, sarà possibile eseguire le notificazioni previste dalla normativa in esame.
3) Il destinatario della notifica tramite PEC dovrà essere un soggetto il cui indirizzo PEC sia inserito in pubblici registri.
4) Il **comma 4 bis dell'articolo 8 della L. 53/94** dispone ora che l'avvocato che voglia notificare telematicamente a mezzo PEC non abbia più l'obbligo di osservare quanto indicato nei precedenti punti 1, 2, 3 e 4 del citato articolo **venendo meno l'obbligo di annotare nel registro cronologico le notificazioni eseguite**.
5) Il campo **"OGGETTO"** della PEC dovrà obbligatoriamente indicare, così come previsto dall'art. 3 bis comma 4 della L. 53/94, la seguente frase:
notificazione ai sensi della legge n. 53 del 1994.

6) L'art. 3 bis comma 5 della L. 53/94 dispone che la PEC debba contenere i seguenti allegati generati su documento informatico separato:

6.1) la **RELATA DI NOTIFICAZIONE** (creata con word, open office ecc. trasformata, senza scansione, direttamente in PDF e firmata digitalmente) nella quale dovranno essere inseriti i seguenti dati:
a) il nome, cognome ed il codice fiscale dell'avvocato notificante;
b) gli estremi del provvedimento autorizzativo del Consiglio dell'Ordine nel cui Albo è iscritto l'avvocato che procede alla notifica;
c) il nome e cognome o la denominazione e ragione sociale ed il codice fiscale della parte che ha conferito la procura alle liti;
d) il nome e cognome o la denominazione e ragione sociale del destinatario;
e) l'indirizzo di posta elettronica certificata a cui l'atto viene notificato;
f) l'indicazione dell'elenco da cui il predetto indirizzo è stato estratto;
g) l'attestazione di conformità (eventuale) di cui al comma 2 dell'art. 3 bis L. 53/94.
h) per le notificazioni effettuate in corso di procedimento deve, inoltre, essere indicato l'ufficio giudiziario, la sezione, il numero e l'anno di ruolo (art. 3 bis comma 6 della L. 53/94**).**
I) una volta ultimata, la relata di notificazione, prima di essere allegata alla PEC, deve essere "firmata" con FIRMA DIGITALE.

6.2) L'ATTO CHE L'AVVOCATO DEVE NOTIFICARE:
ipotizzerò la notifica di atto introduttivo (ad es. citazione).

Nel caso di **ATTO DI CITAZIONE** sarà necessario allegare:

a) l'atto firmato digitalmente dall'avvocato (creato precedentemente con word e direttamente trasformato in file PDF).
Invero la nuova normativa non prevede più, espressamente, che l'atto da notificare sia sottoscritto digitalmente dal professionista prevedendo, invece, che l'avvocato possa procedere alla notifica allegando l'atto nel formato PDF avendo cura di firmare digitalmente la relata di notifica. **Il comma 1 dell'art. 18 precisa però che anche le scansioni da notificare devono essere redatte nei formati consentiti dalle specifiche tecniche del processo telematico le quali prevedono che l'atto del processo sia, tra l'altro, in formato PDF con firma digitale p7m. Pertanto si potrebbe sostenere che la firma digitale del documento informatico contenente la scansione, eliminata dal comma 4 dell'art.18, riviva attraverso il comma 1 (così come, a mio avviso giustamente, sostenuto dal collega Giorgio Rognetta)**[32].
Per tale motivo e per eccesso di scrupolo, suggerisco di firmare digitalmente anche l'atto da notificare e di allegare, eventualmente, alla PEC anche il medesimo atto in formato PDF non sottoscritto digitalmente.

b) la procura alle liti, rilasciata all'avvocato su foglio separato del quale è estratta copia informatica, anche per immagine, ai sensi e per gli effetti dell'art. 18 n. 5 del DM 44/2011 così come modificato dal DM 48/2013. L'avvocato, in siffatta ipotesi, redige tramite software (word, open office ecc.) la procura alle liti, la stampa, la fa sottoscrivere al cliente, la sottoscrive egli

[32] http://www.altalex.com/index.php?idnot=63050

stesso, scansiona successivamente il documento così formato estraendone copia informatica per immagine (PDF) e, prima di allegarla al messaggio PEC, la sottoscrive con firma digitale.
c) la relata di notificazione (per la quale rimando a quanto indicato al precedente punto **6.1**).

7) Prima di inoltrare la PEC l'avvocato dovrà accertarsi di aver selezionato, nella PEC, quale TIPO DI **RICEVUTA DI AVVENUTA CONSEGNA**, quella **COMPLETA**, così come previsto dal comma 6 dell'art. 18 del DM 44/11 così come modificato dal DM 48/2013.

8) Il perfezionamento della notifica.
La **notifica via PEC può dirsi perfezionata per il soggetto notificante, nel momento in cui viene generata la ricevuta di accettazione prevista dall'articolo 6, comma 1, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e, per il destinatario, nel momento in cui viene generata la ricevuta di avvenuta consegna prevista dall'articolo 6, comma 2, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 (art. 3 bis comma 3 della L. 53/94).**
Ricordo che non esistono, per l'avvocato notificatore, le stesse limitazioni territoriali relative agli Ufficiali Giudiziari: la notifica di una citazione avanti il Tribunale di Teramo, da eseguirsi nei confronti di un destinatario residente a Caltanissetta, ben può essere eseguita da un avvocato con studio in Bari.

9) Prova dell'avvenuta notifica.
Nel caso di notifica telematica, la prova dell'avvenuta notifica (tramite deposito negli atti di causa) è costituita dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna completa (ossia da documenti informatici) del messaggio PEC, ma ciò solo se esiste un fascicolo telematico del procedimento.
Quando invece non esiste un fascicolo telematico non è possibile procedere al deposito con modalità telematiche dell'atto notificato a norma dell'art. 3 bis L. 53/94; l'art. 9 comma 1 bis della L. 53/94, introdotto dalla Legge 228/2012, dispone che "*… l'avvocato estrae copia su supporto analogico del messaggio di posta elettronica certificata, dei suoi allegati e della ricevuta di accettazione e di avvenuta consegna e ne attesta la conformità ai documenti informatici da cui sono tratte ai sensi dell'articolo 23, comma 1, del decreto legislativo 7 marzo 2005, n. 82*".
L'avvocato notificatore, pertanto, potrà stampare su carta l'intero messaggio PEC relativo alla notifica, con i suoi allegati e con le ricevute di accettazione e di avvenuta consegna, ed attestare la conformità di tale copia ai documenti informatici originali.

10) Adempimenti fiscali.
L'art. 10 della L. 53/94 prevede che agli atti notificati è apposta, al momento dell'esibizione o del deposito nella relativa procedura, apposita marca, il cui modello e importo sono stabiliti con decreto del Ministro della Giustizia; a tal proposito ricordo che ad oggi è vigente l'art. 2 del DM 27 maggio 1994 il quale prevede che i diritti di notifica siano pari ad Euro 2,58 per le notifiche fino due destinatari, Euro 7,75 per le notifiche da tre a sei destinatari ed Euro 12,40 per le notifiche aventi più di sei destinatari.
Quando l'atto è notificato in via telematica a mezzo PEC, ai sensi dell'art. 3 bis L. 53/94, il pagamento dei diritti di notifica deve avvenire mediante sistema telematico (pagamento telematico delle spese di giustizia).
In caso di violazioni della disposizione di cui all'art. 10 L. 53/94 si applicano le sanzioni previste per l'imposta di bollo, con le stesse modalità e procedure, in quanto applicabili.
Sul punto osservo che:

a) una volta effettuato il pagamento telematico dei diritti di notifica, il sistema rilascia due ricevute (files): una in formato "PDF" e l'altra in formato "XML".
La ricevuta-file in formato "XML" dovrà essere utilizzata, quale allegato, nel caso in cui l'atto notificato venga depositato telematicamente.
La ricevuta-file in formato "PDF" verrà utilizzata, dopo essere stata stampata, quale allegato, nel caso in cui l'atto notificato venga depositato in modalità cartacea.
b) Ad oggi però non tutti gli Uffici Giudiziari sono a valore legale sia per la ricezione di depositi telematici sia per la ricezione dei pagamenti telematici; potrebbe porsi, quindi, il duplice caso in cui da una parte l'Ufficio Giudiziario abbia il valore legale per il deposito telematico degli atti ma non anche quello per l'accettazione dei pagamenti telematici o, dall'altra, la presenza di Ufficio Giudiziario che abbia il valore legale per l'accettazione di pagamenti telematici ma non anche quello per il deposito di atti telematici.
Nel primo caso, eseguita la notifica a mezzo PEC, il deposito della notifica potrebbe avvenire in modalità telematica ma, non accettando l'Ufficio Giudiziario pagamenti telematici, i diritti di notifica dovrebbero comunque essere pagati nella modalità tradizionale (marca lottomatica o F23), e la prova dell'avvenuto pagamento dovrebbe essere depositata nella stessa modalità prevista per il deposito del decreto ingiuntivo telematico; **in tale ipotesi l'avvocato sarebbe nella impossibilità di attenersi a quanto disposto dall'art. 10 L. 53/94 (pagamento telematico dei diritti di notifica).**
Nel secondo caso, eseguita la notifica a mezzo PEC, il deposito della notifica non potrà essere telematico e quindi unitamente al deposito cartaceo della notifica l'avvocato avrà cura di depositare la stampa della ricevuta-file "PDF" ottenuta a seguito di pagamento telematico.
Ritengo doveroso ed opportuno ricordare, da ultimo, che l'avvocato che compila **la relazione o le attestazioni di cui agli articoli 3, 3-bis e 9** o le annotazioni di cui all'articolo 5 della L. 53/94, è considerato pubblico ufficiale ad ogni effetto e che il compimento di irregolarità o abusi nell'esercizio delle facoltà previste dalla legge 53/94 costituisce grave illecito disciplinare, indipendentemente dalla responsabilità prevista da altre norme (art. 6 L. 53/94).

11) Fac simile relata di notifica:

FAC SIMILE RELATA DI NOTIFICA DI ATTO DI CITAZIONE

RELATA DI NOTIFICA A MEZZO DI POSTA ELETTRONICA CERTIFICATA

ex art. 3bis Legge 21 gennaio 1994, n. 53

Io sottoscritto Avvocato _____, con studio in _____ alla Via _____, CF:_____, P.IVA: _____ nella mia qualità di difensore e domiciliatario del Sig. _____, res. in _____ alla Via _____ C.F. _____, giusta procura alle liti che si allega ai sensi dell'art. 83 comma 3 c.p.c., autorizzato alle notifiche ex L. 21 gennaio 1994 n. 53 e succ. mod. giusta autorizzazione del Consiglio dell'Ordine degli Avvocati di _____ del _____ ho

NOTIFICATO

ad ogni effetto di legge copia informatica da me firmata digitalmente dell'atto di citazione prodotto a favore del Sig. _____, CF: _____ e contro

_____, nell'instaurando giudizio civile dinanzi al Tribunale di _____, di cui attesto la conformità all'originale cartaceo ai sensi dell'art. 22 del decreto legislativo del 07 marzo 2005 n. 82, nonché procura alle liti a me rilasciata dal Sig. _____ originariamente su foglio separato dal quale ho estratto copia informatica per immagine, sottoscritta digitalmente, in conformità di quanto previsto dall'art. 18 n. 5 del DM 44/2011 così come modificato dal DM 48/2013 a:

1) ALFABETAGAMMA SPA, con sede in _____ alla Via _____, CF: _____, P.IVA: _____ trasmettendone copia informatica a mezzo posta elettronica certificata all'indirizzo (INSERIRE INDIRIZZO PEC DEL DESTINATARIO) estratto dal registro PEC delle imprese tenuto dal registro delle imprese.

Attesto da ultimo che il messaggio PEC, oltre alla presente relata di notifica sottoscritta digitalmente, contiene i seguenti ulteriori allegati informatici:

1) atto di citazione (sottoscritto digitalmente)

2) procura alle liti (sottoscritta digitalmente)

Luogo _____ data _____

Avv. (NOME E COGNOME AVVOCATO)

FAC SIMILE RELATA DI NOTIFICA DI ATTO DI CITAZIONE IN OPPOSIZIONE A DECRETO INGIUNTIVO

RELATA DI NOTIFICA A MEZZO DI POSTA ELETTRONICA CERTIFICATA

ex art. 3bis Legge 21 gennaio 1994, n. 53

Io sottoscritto Avvocato _____, con studio in _____ alla Via _____, C.F.: _____, P.IVA:_____ nella mia qualità di difensore e domiciliatario del Sig. _____, res. in _____, alla Via _____ C.F. _____, giusta procura alle liti che si allega ai sensi dell'art. 83 comma 3 c.p.c., autorizzato alle notifiche ex L. 21 gennaio 1994 n. 53 e succ. mod. giusta autorizzazione del Consiglio dell'Ordine degli Avvocati di _____ del _____ ho

NOTIFICATO

ad ogni effetto di legge copia informatica da me firmata digitalmente dell'atto di citazione in opposizione al decreto ingiuntivo n. _____ emesso dal Tribunale di _____ notificato il _____ al Sig. _____ proposto dinanzi al Tribunale di _____, a favore del Sig. _____, CF:_____, di cui attesto la conformità all'originale cartaceo ai sensi dell'art. 22 del decreto legislativo del 07 marzo 2005 n. 82, nonché procura alle liti a me rilasciata dal Sig. _____ originariamente su foglio separato dal

quale ho estratto copia informatica per immagine, sottoscritta digitalmente, in conformità di quanto previsto dall'art. 18 n. 5 del DM 44/2011 così come modificato dal DM 48/2013 a:

1) Avvocato _____, residente in _____ alla Via _____, CF: _____, quale procuratore domiciliatario della ALFABETAGAMMA SPA, nella persona del legale rappresentante pro-tempore trasmettendone copia informatica a mezzo posta elettronica certificata all'indirizzo (INSERIRE INDIRIZZO PEC DELL'AVVOCATO DESTINATARIO) estratto dal REGINDE, registro generale degli indirizzi elettronici gestito dal Ministero della Giustizia.

Attesto da ultimo che il messaggio PEC, oltre alla presente relata di notifica sottoscritta digitalmente, contiene i seguenti ulteriori allegati informatici:

1) atto di citazione in opposizione a decreto ingiuntivo (sottoscritto digitalmente)

2) procura alle liti (sottoscritta digitalmente)

Luogo _____ data _____

Avv. (NOME E COGNOME AVVOCATO)

13.3 – Notifica tramite PEC ex L. 53/94 e (impossibile) deposito telematico dell'atto notificato presso l'Ufficio Giudiziario.

L'art. 9 n. 1 L. 53/94, induce a pensare che l'atto notificato dovrebbe essere, di regola, depositato telematicamente; è infatti il successivo n. 2 dello stesso articolo a confermarlo recitando che "Qualora non si possa procedere al deposito con modalità telematiche dell'atto notificato a norma dell'articolo 3-bis, l'avvocato estrae copia su supporto analogico del messaggio di posta elettronica certificata, dei suoi allegati e della ricevuta di accettazione e di avvenuta consegna e ne attesta la conformità ai documenti informatici da cui sono tratte ai sensi dell'articolo 23, comma 1, del decreto legislativo 7 marzo 2005, n. 82".
Abbiamo visto che il tipo di ricevuta da selezionare per la notifica dell'atto a mezzo PEC, è quella completa ed è quindi questa che, telematicamente, deve essere depositata presso la cancelleria dell'Ufficio Giudiziario.
Per far questo altresì deduco che l'avvocato dovrà "salvare" sul proprio PC la ricevuta completa per poi inserirla nella "busta telematica" creata dal "redattore atti" messo a disposizione dei PDA affinché la stessa possa essere depositata telematicamente nel rispetto del DM 44/2011 e delle specifiche tecniche del 18 luglio 2011.
Ma … salvando sul vostro PC una qualsiasi ricevuta completa di PEC inviata, vi accorgerete che l'estensione del file è di tipo **".eml"**.
Bene, l'art. 13 delle specifiche tecniche del 18 luglio 2011 previste dall'art. 34 del DM 44/2011 elenca tassativamente quali siano, ai fini del deposito telematico di atti e/o documenti, i formati di file consentiti:

a) .pdf
b) .odf
c) .rtf
d) .txt

e) .jpg
f) .gif
g) .tiff
h) .xml.

altresì specificando che è consentito l'utilizzo dei seguenti formati compressi **purché contenenti file nei formati previsti indicati dalle lettere da a) a h)**:

a) .zip
b) .rar
c) .arj.

Abbiamo però detto che la RICEVUTA COMPLETA di una PEC inviata viene rilasciata sul nostro PC, dopo averla "salvata", in **formato ".eml".**
Ciò significa che, non essendo il formato ".eml" tra quelli più sopra elencati e non potendosi depositare telematicamente formati diversi da quelli, **ad oggi non è possibile, per nessun avvocato, ottemperare a quanto previsto dall'art. 9 n. 1 L. 53/94, ossia depositare telematicamente la RICEVUTA COMPLETA**!

Si accorge di tale "pasticcio" anche DGSIA che, in data 30 maggio 2013, pubblica il seguente comunicato[33]:

"Con riguardo alla possibilità, per gli avvocati, di procedere alle notifiche via PEC, come disciplinata, da ultimo, dal Decreto del Ministro della Giustizia del 3 aprile 2013 n. 48, pubblicato sulla G.U. n.107 del 9 maggio 2013 (che modifica l'articolo 18 del Decreto del Ministro della Giustizia del 21 febbraio 2011 n.44), si comunica che la Direzione Generale Sistemi informativi Automatizzati, provvederà, dopo aver acquisito i necessari pareri, ad emanare il nuovo provvedimento contenente le specifiche tecniche, che fissano i ***formati consentiti****.*
Tali specifiche riguarderanno anche le modalità di trasmissione in via telematica all'ufficio giudiziario delle ricevute previste dall'articolo 3-bis, comma 3, della legge 53/94, nonché della copia dell'atto notificato, ai sensi dell'articolo 9, comma 1, della medesima legge".

E' facilmente intuibile che il futuro provvedimento del Ministero della Giustizia dovrebbe avere quale fine quello di individuare:
1) le specifiche tecniche idonee a fissare i FORMATI CONSENTITI (modificando quindi le specifiche tecniche del 18 luglio 2011 così come previste dall'art. 34 del DM 44/2011);
2) le modalità di trasmissione in via telematica all'Ufficio Giudiziario delle ricevute previste dall'art. 3 bis comma 3 L. 53/94
3) le modalità della copia dell'atto notificato ai sensi dell'art. 9, comma 1, della L. 53/94.
Dovrà necessariamente modificare il contenuto dell'art. 13 delle specifiche tecniche del 18 luglio 2011 previste dall'art. 34 del DM 44/2011 inserendo nell'elenco dei formati dei file consentiti ai fini del deposito telematico di atti e/o documenti anche il formato ".eml" per consentire all'avvocato il deposito telematico della RICEVUTA COMPLETA della notifica effettuata tramite PEC.

[33] http://pst.giustizia.it/PST/it/pst_3_1.wp?previousPage=homepage&contentId=NEW737

Se in effetti quanto dedotto è giusto, due domande sorgono spontanee:
possibile che coloro che hanno elaborato il DM 48/2013 non siano accorti che, oltre alle modifiche introdotte bisognava aggiungere anche quella dell'art. 13 delle specifiche tecniche del 18 luglio 2011 previste dall'art. 34 del DM 44/2011?
Possibile che, arrivati ormai alla fine di ottobre 2013, il nuovo provvedimento (annunciato il 30 maggio 2013) non sia stato ancora emanato da DGSIA?
Vorrei e potrei dire molte cose ma preferisco limitarmi ad un semplice … no comment!

13.4 - Notifiche avvocati tramite PEC L. 53/94: dubbi circa l'effettiva possibilità del loro utilizzo prima del 15 dicembre 2013.

Da più parti si sostiene che, nonostante la pubblicazione del DM 48/13, per notificare avvalendosi della PEC gli avvocati dovrebbero comunque attendere il 15 dicembre 2013 e ciò in riferimento a quanto previsto dall'art. 16 ter L. 17.12.2012 n. 221, che per comodità trascrivo:

Legge 17 dicembre 2012 n. 221
Art. 16-ter. Pubblici elenchi per notificazioni e comunicazioni
(introdotto dall'art. 1, comma 19, numero 2), L. 228/2012)

1. A decorrere dal 15 dicembre 2013, ai fini della notificazione e comunicazione degli atti in materia civile, penale, amministrativa e stragiudiziale si intendono per pubblici elenchi quelli previsti dagli articoli 4 e 16, comma 12, del presente decreto; dall'articolo 16 del decreto-legge 29 novembre 2008, n. 185, convertito con modificazioni dalla legge 28 gennaio 2009, n. 2, dall'articolo 6-bis del decreto legislativo 7 marzo 2005, n. 82, nonché il registro generale degli indirizzi elettronici, gestito dal ministero della giustizia.

Ad avviso di molti, come detto, il contenuto del trascritto articolo impedirebbe, oggi, al professionista di avvalersi della PEC per le notifiche ex L. 53/94 in quanto, solo a decorrere dal 15 dicembre 2013 potrebbero essere definibili pubblici gli elenchi previsti: dagli articoli 4 e 16, comma 12, della citata norma, dall'articolo 16 del decreto-legge 29 novembre 2008, n. 185, convertito con modificazioni dalla legge 28 gennaio 2009, n. 2, dall'articolo 6-bis del decreto legislativo 7 marzo 2005, n. 82, nonché il registro generale degli indirizzi elettronici, gestito dal ministero della giustizia (REGINDE); per tale motivo sarebbe impossibile per l'avvocato notificare a mezzo PEC prima del 15 dicembre 2013.

A mio modesto e sommesso avviso la norma deve essere invece interpretata nel senso che dal giorno 15 dicembre 2013 solo ed esclusivamente quelli tassativamente indicati dall'art. 16 ter dovranno essere intesi come elenchi pubblici e ciò per attestare con assoluta certezza che successivamente a quella data non possano essere considerati e utilizzati altri pubblici elenchi ai fini dell'estrapolazione dell'indirizzo di posta elettronica certificata del destinatario per le notifiche da effettuarsi tramite PEC.

Ciò significa che da subito gli elenchi che già sono pubblici (con ciò dovendosi intendere quelli gestiti dalla pubblica amministrazione e non solo quelli consultabili da un pubblico indeterminato) per legge (tra questi il REGINDE, il registro imprese e il registro INI-PEC consultabile dal 19 giugno 2013) possono essere utilizzati dall'avvocato per estrapolare l'indirizzo PEC del professionista o di altro soggetto tenuto alla comunicazione obbligatoria del citato indirizzo con la conseguente possibilità di notificare al predetto indirizzo atti a mezzo PEC così come previsto dalla Legge 53/94.

Se l'interpretazione non fosse questa non solo da una lato bisognerebbe aspettare per le notifiche a mezzo PEC il 15 dicembre 2013 ma, dall'altro, significherebbe dubitare che anche il REGINDE fino quella data (15 dicembre 2013) non potrebbe essere utilizzato per reperire gli indirizzi PEC dei professionisti e, conseguentemente, tutti i biglietti di cancelleria sino ad oggi esclusivamente inoltrati telematicamente tramite PEC (comunicazioni telematiche di cancelleria civili e penali) da tutti gli Uffici Giudiziari sarebbero assolutamente privi di efficacia con conseguenze a dir poco catastrofiche per i procedimenti civili e penali a cui gli stessi si riferiscono.
D'altra parte, che il REGINDE ad oggi sia un pubblico elenco (nel significato sopra specificato) lo certifica, implicitamente, l'art. 16 L. 17.12.2012 n. 221:

Art. 16 Legge 17 dicembre 2012 n. 221
Biglietti di cancelleria, comunicazioni e notificazioni per via telematica.

[omissis]

4. Nei procedimenti civili le comunicazioni e le notificazioni a cura della cancelleria sono effettuate esclusivamente per via telematica all'indirizzo di posta elettronica certificata risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni, secondo la normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Allo stesso modo si procede per le notificazioni a persona diversa dall'imputato a norma degli articoli 148, comma 2-bis, 149, 150 e 151, comma 2, del codice di procedura penale. La relazione di notificazione è redatta in forma automatica dai sistemi informatici in dotazione alla cancelleria.

[omissis]

Per cui … se il REGINDE è già oggi per legge idoneo a far si che dallo stesso possano essere estrapolati gli indirizzi PEC dei professionisti per l'inoltro delle comunicazioni di cancelleria non si comprende come lo stesso non possa allo stesso modo essere utilizzato per le notifiche degli avvocati tramite PEC.
Aggiungo poi che, ove fosse stata intenzione del legislatore quella di differire al 15 dicembre 2013 la possibilità per gli avvocati di notificare atti a mezzo PEC, lo stesso avrebbe formalmente esplicitato in maniera chiara tale volontà nella stessa maniera in cui aveva inequivocabilmente posticipato l'entrata in vigore delle modifiche introdotte con la legge 24 dicembre 2012 n. 228 (relative alla notifica tramite PEC L. 53/94)) solo dopo la pubblicazione nella Gazzetta Ufficiale del decreto previsto dal numero 2 dell'art. 16 quater con il quale sarebbe stato modificato l'art. 18 delle regole tecniche previste dal DM 44/2011.
E' naturale che questo è solo un parere per cui la mia posizione sul punto non equivale a certezza anche perché solo chi non ha mai avuto a che fare con il "mondo Giustizia" è in grado, oggi, di dare certezze; ne consegue che, naturalmente, da una parte declino ogni mia responsabilità qualora si pervenga, in maniera certa ed ufficiale, ad una interpretazione diversa dalla mia e, dall'altra, è inutile dirvi che, personalmente, non ho aspettato il 15 dicembre 2013 per notificare tramite PEC.
Sull'argomento segnalo l'articolo a firma dell'amico e collega Carlo Piana che, nel commentare[34] una ordinanza del Tribunale di Padova, giunge a conclusioni simili a quelle da me sopra riportate.

[34] http://www.dirittoegiustizia.it/news/8/0000063341/Notifiche_via_PEC_altre_decisioni_astruse.html

CAPITOLO XIV
I Vademecum del Processo Telematico

Sommario: Premessa - 14.1. Vademecum per il deposito telematico del ricorso per decreto ingiuntivo – 14.2. Vademecum per il deposito telematico della comparsa di costituzione e risposta – 14.3. Vademecum per il deposito telematico delle memorie ex art. 183 n. 6 c.p.c. telematico. – 14.4. Vademecum per il deposito telematico della comparsa conclusionale – 14.5. Vademecum per il deposito telematico dell'istanza di ammissione al passivo fallimentare.

Premessa.
sperando di fare cosa utile e gradita ho predisposto, sulla base delle prassi in uso nei diversi Uffici Giudiziari, brevi vademecum relativi al deposito telematico dei seguenti atti:
ricorso per decreto ingiuntivo, comparsa di costituzione e risposta, memorie ex art. 183 n. 6 c.p.c., comparsa conclusionale e replica e istanza di ammissione al passivo fallimentare.
Le espressioni utilizzate sono volutamente poco tecniche affinchè il contenuto possa essere compreso anche da chi non ha confidenza con lo strumento informatico.
Non posso escludere che, in alcuni Uffici Giudiziari siano adottate procedure parzialmente difformi dal quelle qui indicate; per tale motivo consiglio al professionista di verificare, presso l'Ufficio Giudiziario competente a ricevere il deposito telematico, l'esistenza di modalità diverse.
Declino, da ultimo, ogni responsabilità per errori e/o danni che possano verificarsi per aver fatto affidamento sulle informazioni contenute nei vademecum.

14.1 - Vademecum per il deposito telematico del ricorso per decreto ingiuntivo.
Il ricorso per decreto ingiuntivo telematico deve essere redatto con il software tradizionalmente utilizzato dall'avvocato (Word, Open Office, ecc.) e trasformato nel formato **"PDF TESTO"** senza scansione; chi usa Open Office, può creare il file **"pdf testo"** cliccando sul tasto **"pdf"** presente nella barra degli strumenti; chi usa Word 2010 o versioni più recenti può salvare il documento in formato PDF utilizzando la funzione presente in **"salva con nome"**, chi invece usa altri programmi che non consentono quanto sopra indicato **può "stamparlo in pdf" con stampante virtuale** usando, ad esempio, il programma gratuito "**PDF CREATOR**" o **"PDF24"** o similari; è necessario, naturalmente, verificare di aver installato sul proprio computer una **stampante virtuale PDF (**"**PDF CREATOR**" o **"PDF24"** o similari**)**. Dal menu **FILE > STAMPA > selezionare la stampante PDF > OK > salvare il file PDF in qualsiasi cartella del computer.** Questo è il file da allegare come **"atto introduttivo"** nella fase di creazione della busta.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").
Una volta ottenuto il file PDF, l'avvocato dovrà sottoscriverlo tramite firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.
Il ricorso deve contenere, naturalmente, i **nomi delle parti**, il **codice fiscale dell'avvocato** ed il suo indirizzo di **posta elettronica certificata** nonché **il codice fiscale o la partita iva del cliente**. Le imprese devono essere individuate tramite la relativa ragione sociale e le espressioni "Ditta" e/o "Società" devono essere premesse solo nell'ipotesi in cui siano comprese nella ragione sociale. Le abbreviazioni (ad esempio: spa, snc, ecc.) devono essere inserite senza puntini tra le singole lettere.

Nel predisporre il ricorso **non deve essere redatto ed inoltrato il provvedimento di ingiunzione del giudice** in quanto questo sarà redatto dal magistrato utilizzando il software messo a sua disposizione dal Ministero.

La **PROCURA ALLE LITI** può essere rilasciata a margine del ricorso o con atto separato:
PROCURA A MARGINE DEL RICORSO: l'avvocato dovrà stampare la prima pagina del ricorso e, successivamente, la stessa dovrà essere sottoscritta dal cliente per il conferimento del mandato e sottoscritta con firma autografa dall'avvocato. La procura poi, dovrà essere trasformata in file "PDF immagine" tramite scanner e, successivamente il file PDF ottenuto dovrà essere firmato tramite firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").
PROCURA RILASCIATA CON ATTO SEPARATO: la stessa deve contenere tutti gli elementi affinchè si possa evincere per quale tipo di atto è conferita (ad esempio: ricorso per decreto ingiuntivo a favore di Caio contro Sempronio per il pagamento di Euro 20.000,00 da depositarsi presso il Tribunale di XXXXXXXXX); dopo averla stampata deve essere sottoscritta dal cliente per il conferimento del mandato e sottoscritta con firma autografa dall'avvocato.
La procura poi, dovrà essere trasformata in file "PDF immagine" tramite scanner ed il file PDF ottenuto dovrà essere firmato con firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.

I **DOCUMENTI cartacei** da allegare al ricorso **dovranno essere trasformati**, mediante scanner, **in file "PDF immagine" (suggerisco che ad ogni documento cartaceo corrisponda un file PDF avente quale nome quello del documento)**; non è necessario sottoscrivere i documenti con firma digitale a meno che ciò non sia richiesto dalla tipologia del documento. I documenti vanno scansionati **IN BIANCO E NERO** e a **BASSA RISOLUZIONE** (suggerisco 100 dpi). Eventuali fotografie in formato digitale .jpeg o .bmp devono essere trasformate in PDF aprendo il relativo file e "stampandole" in pdf seguendo la procedura di cui sopra.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").

La **NOTA SPESE** deve essere redatta con il software tradizionalmente utilizzato dall'avvocato (word, open office ecc. ecc.) e trasformata in "PDF testo" senza scansione utilizzando la stessa procedura indicata per la redazione del ricorso; una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo con firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").
Dovrà, in ultimo, essere predisposto l'**INDICE DEI DOCUMENTI** allegati al ricorso; il detto indice deve essere redatto con il software tradizionalmente utilizzato dall'avvocato (word, open office ecc.) e trasformato in "PDF TESTO" senza scansione utilizzando la stessa procedura indicata per la redazione del ricorso; una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo con firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura

solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").

Se il **CLIENTE E' ASSISTITO DA DUE AVVOCATI**, l'avvocato che redige il ricorso dovrà inserire il nominativo del collega sia nel ricorso sia in sede di compilazione della **"BUSTA"** mediante il "**REDATTORE DI ATTI PCT PRESENTE NEL PDA"** e apporrà la sua firma digitale (è possibile apporre all'atto anche più di una sottoscrizione digitale ma, a tal proposito, per esperienza diretta, posso affermare che, qualora l'atto venga sottoscritto digitalmente da due avvocati, il sistema genera un errore all'esito dei controlli automatici; lo stesso successivamente, viene però accettato dalla cancelleria). Così procedendo la cancelleria potrà consentire ai predetti avvocati sia la ricezione delle comunicazioni telematiche sia la consultazione del fascicolo con "**POLISWEB PCT"**.

LA NOTA DI ISCRIZIONE A RUOLO:
solitamente la maggior parte dei "**REDATTORI DI ATTI PCT PRESENTI NEI PDA"** consentono di crearla automaticamente utilizzando i dati inseriti dall'avvocato per la creazione del fascicolo; è comunque sempre possibile redigerla con il software tradizionalmente utilizzato dall'avvocato, scansionarla in PDF, sottoscriverla digitalmente e allegarla al ricorso nella fase di creazione della **BUSTA** specificando come tipo di allegato: **NOTA DI ISCRIZIONE A RUOLO**.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").

CONTRIBUTO UNIFICATO:
se il pagamento viene effettuato con i metodi tradizionali il contributo unificato va acquisito tramite scanner e allegato al ricorso dando come nome al file **"CONTRIBUTO UNIFICATO"**. Nel caso di pagamento effettuato tramite **Lottomatica** va scansionata la marca apposta sull'apposito modulo già in uso.
Nel caso di pagamento effettuato tramite **F23** va scansionato il modulo relativo.
A tal proposito si segnala che la maggior parte degli Uffici Giudiziari prevede che, ove il pagamento del contributo unificato avvenga nei modi tradizionali, lo stesso **debba essere versato unicamente tramite F23.**
Negli Uffici Giudiziari abilitati è possibile effettuare il pagamento del contributo unificato telematicamente ottenendo in tempo reale la ricevuta telematica di pagamento (RT) stamparla o scaricarla sul proprio computer in formato elettronico, **PDF** o **XML**, in base alla modalità attivata dal Ministero della Giustizia presso l'Ufficio Giudiziario.
La RT (ricevuta telematica) in **PDF** deve essere inserita come allegato nella busta telematica relativa al deposito da effettuare mediante l'apposita funzione presente nel **PDA**.
La RT (ricevuta telematica) in formato **XML** dovrà essere inserita come allegato nella busta telematica relativa al deposito da effettuare mediante l'apposita funzione presente nel **PDA**.
Ultimata la **BUSTA** (contenente il ricorso e tutti gli allegati sopra citati e che, si ricorda, non dovrà superare i 30 MB) la stessa dovrà essere inviata mediante **PDA** tramite **PEC** all'Ufficio Giudiziario competente; successivamente all'avvocato verranno inviate, nella propria casella di posta elettronica certificata, quattro ricevute:

RICEVUTA DI ACCETTAZIONE
RICEVUTA DI CONSEGNA
RICEVUTA ESITI CONTROLLI AUTOMATICI

RICEVUTA DI DEFINITIVA ACQUISIZIONE, DA PARTE DEL CANCELLIERE, DEL RICORSO E DEGLI ALLEGATI.

14.2 - Vademecum per il deposito telematico della comparsa di costituzione e risposta.

Per depositare telematicamente la **COMPARSA DI COSTITUZIONE E RISPOSTA** la stessa deve essere redatta con il software tradizionalmente utilizzato dall'avvocato (Word, Open Office, ecc.) e trasformata in "PDF TESTO" senza scansione; chi usa Open Office, può creare il file pdf cliccando sul tasto **"pdf"** presente nella barra degli strumenti; chi usa Word 2010 può salvare la comparsa in formato PDF utilizzando la funzione presente in **"salva con nome"**, chi invece usa altri programmi che non consentono quanto sopra indicato **può "stamparla in pdf" con stampante virtuale** usando, ad esempio, il programma gratuito "**PDF CREATOR**" o **"PDF24"** o similari; è necessario, naturalmente, verificare di aver installato sul proprio computer una **stampante virtuale PDF (**"**PDF CREATOR**" o **"PDF24"** o similari**)**. Dal menu **FILE > STAMPA > selezionare la stampante PDF > OK > salvare il file PDF in qualsiasi cartella del computer.** Questo è il file da allegare come **"atto successivo"** nella fase di creazione della busta.

La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").

Una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo tramite firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.

Se il **CLIENTE E' ASSISTITO DA DUE AVVOCATI**, l'avvocato che redige la comparsa di costituzione dovrà inserire il nominativo del collega sia nella comparsa sia in sede di compilazione della **"BUSTA"** mediante il "**REDATTORE DI ATTI PCT PRESENTE NEL PDA"** e apporrà la sua firma digitale (è possibile apporre all'atto anche più di una sottoscrizione digitale ma, a tal proposito, per esperienza diretta, posso affermare che, qualora l'atto venga sottoscritto digitalmente da due avvocati, il sistema genera un errore all'esito dei controlli automatici; lo stesso successivamente, viene però accettato dalla cancelleria). Così procedendo la cancelleria potrà consentire ai predetti avvocati sia la ricezione delle comunicazioni telematiche sia la consultazione del fascicolo con "**POLISWEB PCT"**.

La comparsa di costituzione deve contenere, naturalmente, i **nomi delle parti**, il **codice fiscale dell'avvocato** ed il suo indirizzo di **posta elettronica certificata** nonché **il codice fiscale o la partita iva del cliente**. Le imprese devono essere individuate tramite la relativa ragione sociale e le espressioni "Ditta" e/o "Società" devono essere premesse solo nell'ipotesi in cui siano comprese nella ragione sociale. Le abbreviazioni (ad esempio: spa, snc, ecc.) devono essere inserite senza puntini tra le singole lettere.

La **PROCURA ALLE LITI** può essere rilasciata a margine della comparsa di costituzione o con atto separato:

PROCURA A MARGINE DELLA COMPARSA: l'avvocato dovrà stampare la prima pagina della comparsa e, successivamente, la stessa dovrà essere sottoscritta dal cliente per il conferimento del mandato e sottoscritta con firma autografa dall'avvocato. La procura poi, dovrà essere trasformata in file "PDF immagine" tramite scanner e, successivamente il file PDF ottenuto dovrà essere firmato tramite firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.

La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").

PROCURA RILASCIATA CON ATTO SEPARATO: la stessa deve contenere tutti gli elementi affinchè si possa evincere per quale tipo di atto è conferita (ad esempio: comparsa di costituzuine e risposta a favore di Caio contro Sempronio nel procedimento civile pendente dinanzi al Tribunale di XXXXXXXX iscritto al nr. _____); dopo averla stampata deve essere sottoscritta dal cliente per il conferimento del mandato e sottoscritta con firma autografa dall'avvocato.
La procura poi, dovrà essere trasformata in file "PDF immagine" tramite scanner e, successivamente il file PDF ottenuto dovrà essere firmato tramite firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.

I **DOCUMENTI cartacei** da allegare alla comparsa **dovranno essere trasformati**, mediante scanner, **in file "PDF immagine" (suggerisco che ad ogni documento corrisponda un file PDF avente quale nome quello del documento)**; non è necessario sottoscrivere i documenti con firma digitale a meno che ciò non sia richiesto dalla tipologia del documento. I documenti vanno scansionati **IN BIANCO E NERO** e a **BASSA RISOLUZIONE** (suggerisco 100 dpi). Eventuali fotografie in formato digitale .jpeg o .bmp possono essere così allegate o trasformate in pdf aprendo il relativo file e "stampandole virtualmente" seguendo la procedura sopra descritta.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").

La DICHIARAZIONE DI VALORE:
in ottemperanza a quanto previsto dalla normativa sul contributo unificato, insieme agli altri documenti deve essere redatta e depositata la dichiarazione di valore.
Tale dichiarazione deve essere redatta con il software tradizionalmente utilizzato dall'avvocato (word, open office ecc.) e trasformato in "PDF TESTO" senza scansione utilizzando la stessa procedura indicata per la redazione della comparsa; una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo tramite firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").
Dovrà, in ultimo, essere predisposto l'**INDICE DEI DOCUMENTI** allegati alla comparsa di costituzione e risposta; il detto indice deve essere redatto con il software tradizionalmente utilizzato dall'avvocato (word, open office ecc.) e trasformato in PDF senza scansione utilizzando la stessa procedura indicata per la redazione della comparsa; una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo tramite firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?"
Se il **CLIENTE E' ASSISTITO DA DUE AVVOCATI**, l'avvocato che redige la comparsa dovrà inserire il nominativo del collega sia nella comparsa sia in sede di compilazione della **"BUSTA"** mediante il "**REDATTORE DI ATTI PCT PRESENTE NEL PDA"** e apporrà la sua firma digitale (il sistema non consente l'apposizione di più di una firma); a tal proposito, per esperienza diretta, posso affermare che, qualora l'atto venga sottoscritto digitalmente da due avvocati, pur generando il sistema un errore all'esito dei controlli automatici, lo stesso verrà accettato dalla cancelleria). Così procedendo la cancelleria potrà consentire ai predetti avvocati sia la ricezione delle comunicazioni tramite PEC sia la consultazione del fascicolo con "**POLISWEB PCT"**.

CONTRIBUTO UNIFICATO:
ove il contenuto della comparsa di costituzione e risposta sia tale da comportare l'integrazione del contributo unificato già versato da parte attrice, se il pagamento dell'integrazione viene effettuato con i metodi tradizionali il contributo unificato va acquisito tramite scanner e allegato al ricorso dando come nome al file **"CONTRIBUTO UNIFICATO"**. Nel caso di pagamento tramite **Lottomatica** va scansionata la marca apposta sull'apposito modulo già in uso. Nel caso di pagamento tramite **F23** va scansionato il modulo relativo.
A tal proposito si segnala che la maggior parte degli Uffici Giudiziari prevede che, ove il pagamento del contributo unificato avvenga nei modi tradizionali, lo stesso **debba essere versato unicamente tramite F23.**
Negli Uffici Giudiziari abilitati è possibile effettuare il pagamento del contributo unificato telematicamente ottenendo in tempo reale la ricevuta telematica di pagamento (RT) stamparla o scaricarla sul proprio computer in formato elettronico, **PDF** o **XML**, in base alla modalità attivata dal Ministero della Giustizia presso l'Ufficio Giudiziario.
La RT (ricevuta telematica) in **PDF** deve essere inserita come allegato nella busta telematica relativa al deposito da effettuare mediante l'apposita funzione presente nel **PDA**.
La RT (ricevuta telematica) in formato **XML** dovrà essere inserita come allegato nella busta telematica relativa al deposito da effettuare mediante l'apposita funzione presente nel **PDA**.
Ultimata la **BUSTA** (contenente il ricorso e tutti gli allegati sopra citati e che, si ricorda, non dovrà superare i 30 MB) la stessa dovrà essere inviata mediante **PDA** tramite **PEC** all'Ufficio Giudiziario competente; successivamente all'avvocato verranno inviate, nella propria casella di posta elettronica certificata, quattro ricevute:

RICEVUTA DI ACCETTAZIONE
RICEVUTA DI CONSEGNA
RICEVUTA ESITI CONTROLLI AUTOMATICI
RICEVUTA DI DEFINITIVA ACQUISIZIONE, DA PARTE DEL CANCELLIERE, DELLA COMPARSA DI COSTITUZIONE E RISPOSTA E DEGLI ALLEGATI.

14.3 - Vademecum per il deposito telematico delle memorie ex art.183 c.p.c. 6° comma.

Le **MEMORIE EX ART. 183 C.P.C. 6° COMMA** devono essere redatte con il software tradizionalmente utilizzato dall'avvocato (Word, Open Office, ecc.) e trasformate in "PDF TESTO" senza scansione; chi usa Open Office, può creare il file pdf cliccando sul tasto **"pdf"** presente nella barra degli strumenti; chi usa Word 2010 può salvare la memoria in formato PDF utilizzando la funzione presente in **"salva con nome"**, chi invece usa altri programmi che non consentono quanto sopra indicato **può "stamparlo in pdf" con stampante virtuale** usando, ad esempio, il programma gratuito "**PDF CREATOR**" o **"PDF24"** o similari; è necessario, naturalmente, verificare di aver installato sul proprio computer una **stampante virtuale PDF (**"**PDF CREATOR**" o **"PDF24"** o similari**)**. Dal menu **FILE > STAMPA > selezionare la stampante PDF > OK > salvare il file PDF in qualsiasi cartella del computer.** Questo è il file da allegare come **"ATTO SUCCESSIVO"** nella fase di creazione della busta.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").
Una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo tramite firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.

Gli eventuali **DOCUMENTI cartacei** da allegare alla memoria **dovranno essere trasformati**, mediante scanner, **in file "PDF immagine" (suggerisco che ad ogni documento corrisponda un file PDF avente quale nome quello del documento)**; non è necessario sottoscrivere i documenti con firma digitale a meno che ciò non sia richiesto dalla tipologia del documento. I documenti vanno scansionati **IN BIANCO E NERO** e a **BASSA RISOLUZIONE** (suggerisco 100 dpi). Eventuali fotografie in formato digitale jpeg o bmp devono essere trasformate in pdf aprendo il relativo file e "stampandole virtualmente" in pdf seguendo la procedura di cui sopra.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").
Se la memoria prevede il deposito di documenti dovrà, in ultimo, essere predisposto l'**INDICE DEI DOCUMENTI** allegati; il detto indice deve essere redatto con il software tradizionalmente utilizzato dall'avvocato (word, open office ecc.) e trasformato in PDF senza scansione utilizzando la stessa procedura indicata per la redazione della memoria; una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo tramite firma digitale; la firma digitale potrà essere apposta anche avvalendosi dell'apposita opzione proposta dal software di realizzazione della "busta" telematica.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").

Se il **CLIENTE E' ASSISTITO DA DUE AVVOCATI**, l'avvocato che redige la memoria dovrà inserire il nominativo del collega sia nella memoria sia in sede di compilazione della **"BUSTA"** mediante il "**REDATTORE DI ATTI PCT PRESENTE NEL PDA"** e apporrà la sua firma digitale (è possibile apporre all'atto anche più di una sottoscrizione digitale ma, a tal proposito, per esperienza diretta, posso affermare che, qualora l'atto venga sottoscritto digitalmente da due avvocati, il sistema genera un errore all'esito dei controlli automatici; lo stesso successivamente, viene però accettato dalla cancelleria).
Ultimata la **BUSTA** (contenente la memoria e tutti gli allegati sopra citati e che, si ricorda, non dovrà superare i 30 MB) la stessa dovrà essere inviata mediante **PDA** tramite **PEC** all'Ufficio Giudiziario competente; successivamente all'avvocato verranno inviate, nella propria casella di posta elettronica certificata, quattro ricevute:

RICEVUTA DI ACCETTAZIONE
RICEVUTA DI CONSEGNA
RICEVUTA ESITI CONTROLLI AUTOMATICI
RICEVUTA DI DEFINITIVA ACQUISIZIONE, DA PARTE DEL CANCELLIERE, DELLA MEMORIA E DEGLI ALLEGATI.

14.4 - Vademecum per il deposito telematico della comparsa conclusionale.
Per depositare telematicamente la **COMPARSA CONCLUSIONALE** la stessa deve essere redatta con il software tradizionalmente utilizzato dall'avvocato (Word, Open Office, ecc.) e trasformata in file "PDF TESTO" senza scansione; chi usa Open Office, può creare il file pdf cliccando sul tasto **"pdf"** presente nella barra degli strumenti; chi usa Word 2010 può salvare il documento in formato PDF utilizzando la funzione presente in **"salva con nome"**, chi invece usa altri programmi che non consentono quanto sopra indicato **può "stamparlo in pdf" con stampante virtuale** usando, ad esempio, il programma gratuito "**PDF CREATOR**" o **"PDF24"** o similari; è necessario, naturalmente, verificare di aver installato sul proprio computer una **stampante virtuale PDF (**"**PDF CREATOR**" o **"PDF24"** o similari**)**. Dal menu **FILE > STAMPA > selezionare la stampante PDF > OK > salvare il file PDF in qualsiasi cartella del computer.** Questo è il file da allegare come "atto successivo" nella fase di creazione della busta telematica.

La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").
Una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo tramite firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.

La **NOTA SPESE** deve essere redatta con il software tradizionalmente utilizzato dall'avvocato (word, open office ecc. ecc.) e trasformata in PDF senza scansione utilizzando la stessa procedura indicata per la redazione del ricorso; una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo tramite firma digitale; la firma digitale potrà essere apposta anche successivamente avvalendosi della procedura solitamente presente nel software **"REDATTORE ATTI"** che consente di creare la "busta" telematica.
La denominazione del file non dovrà contenere caratteri speciali (lettere accentate, apostrofo oppure altri simboli quali "!$£%&()?").

Se il **CLIENTE E' ASSISTITO DA DUE AVVOCATI**, l'avvocato che redige la comparsa conclusionale dovrà inserire il nominativo del collega sia nella comparsa sia in sede di compilazione della **"BUSTA"** mediante il "**REDATTORE DI ATTI PCT PRESENTE NEL PDA"** e apporrà la sua firma digitale (è possibile apporre all'atto anche più di una sottoscrizione digitale ma, a tal proposito, per esperienza diretta, posso affermare che, qualora l'atto venga sottoscritto digitalmente da due avvocati, il sistema genera un errore all'esito dei controlli automatici; lo stesso successivamente, viene però accettato dalla cancelleria).
Ultimata la **BUSTA** (contenente la comparsa conclusionale e la nota spese e che, si ricorda, non dovrà superare i 30 MB) la stessa dovrà essere inviata mediante **PDA** tramite **PEC** all'Ufficio Giudiziario competente; successivamente all'avvocato verranno inviate, nella propria casella di posta elettronica certificata, quattro ricevute:

RICEVUTA DI ACCETTAZIONE
RICEVUTA DI CONSEGNA
RICEVUTA ESITI CONTROLLI AUTOMATICI
RICEVUTA DI DEFINITIVA ACQUISIZIONE, DA PARTE DEL CANCELLIERE, DELLA COMPARSA CONCLUSIONALE E DEGLI ALLEGATI.

14.5 - Vademecum per il deposito telematico dell'istanza di ammissione al passivo fallimentare.
L'**istanza per l'ammissione al passivo fallimentare** da depositare telematicamente, deve essere redatta con il metodo tradizionale (word, open office ecc. ecc.) e trasformata in "PDF testo" senza scansione; una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo tramite firma digitale.
La **PROCURA ALLE LITI** (**allegato 01**) deve essere rilasciata su foglio separato dall'istanza; dopo averla stampata deve essere sottoscritta dal cliente per il conferimento del mandato e sottoscritta con firma autografa dall'avvocato.
La procura poi, una volta così sottoscritta, dovrà essere trasformata in file "PDF immagine" tramite scanner e, successivamente il file PDF ottenuto dovrà essere firmato tramite firma digitale.
I **DOCUMENTI** cartacei da allegare all'istanza dovranno essere trasformati, mediante scanner, in file PDF. Non è assolutamente necessario sottoscrivere i documenti con firma digitale.
Dovrà essere predisposta una **AUTOCERTIFICAZIONE** (**allegato 02**) con la quale l'avvocato attesta di essere in possesso di tutta la documentazione allegata, in formato PDF, alla domanda di ammissione allo stato passivo del Fallimento. La detta autocertificazione deve essere redatta con il

metodo tradizionale (word, open office ecc. ecc.) e trasformata in "PDF testo" senza scansione; una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo tramite firma digitale.
Dovrà, in ultimo, essere predisposto l'**INDICE DEI DOCUMENTI** allegati all'istanza; il detto indice deve essere redatto con il metodo tradizionale (word, open office ecc. ecc.) e trasformata in "PDF testo" senza scansione; una volta ottenuto il file PDF l'avvocato dovrà sottoscriverlo tramite firma digitale.
Da ultimo, l'istanza di ammissione al passivo, la procura alle liti, l'autocertificazione, i documenti e l'indice dei documenti dovranno essere inviati, quali allegati, dalla PEC dell'avvocato alla PEC indicata dal Curatore nella comunicazione ex art. 92 L.F.

ALLEGATO 01)

Procura ad litem

Io sottoscritta **_____**, nata a _____ il _____ e residente in _____ C.F.: _____**,** delego a rappresentarmi e difendermi, in ogni stato e grado della procedura avente ad oggetto istanza di ammissione al passivo fallimentare _____ con tutti i poteri di cui all' art. 84 c.p.c., eventuali giudizi di garanzia, relativi procedimenti esecutivi con le facoltà inerenti al mandato alle liti, l'**Avvocato _____** del foro di _____, eleggendo domicilio presso il suo studio, sito in _____ (__), alla Via _____**.**
Dichiaro altresì di essere stata debitamente informata dei diritti a me spettanti ed autorizzo, in base al D.Lvo n. 196/2003 il trattamento dei dati personali ivi compresi quelli sensibili.
_____, lì _____ ottobre 2013

_____ (firma autografa della parte):

E' autentica la firma che precede

Avv. _____: (firma autografa avvocato)

Atto firmato digitalmente dall'Avv. _____.

ALLEGATO 02)

AUTOCERTIFICAZIONE
(D.P.R. 445 del 28 dicembre 2000)

Il sottoscritto Avv. _____, nato a _____ il giorno _____, residente in _____ (___), alla Via _____, con studio in _____ (__) alla Via _____, C.F. _____, quale difensore del_____, nato a _____ il _____ e residente in _____ C.F.: _____ giusta procura rilasciata in data _____ con atto separato, consapevole delle sanzioni penali, nel caso di dichiarazioni mendaci, di formazione o uso di atti falsi, richiamate dall'art. 76 D.P.R. 445 del 28 dicembre 2000,

DICHIARA

di essere in possesso di tutta la documentazione in originale evidenziata ed allegata alla domanda di ammissione allo stato passivo del Fallimento _____ (Reg. Fall. n. _____) del _____ - Giudice delegato: _____ - Curatore: Dott. _____ la cui udienza per l'adunanza di approvazione dello stato passivo è fissata per il giorno

_____ e di essere disponibile a esibirla dietro semplice richiesta degli organi di procedura.
_____ _____ ottobre 2013

Avv. _____:

Atto firmato digitalmente dall'Avv. _____.

CAPITOLO XV
Sette consigli per il professionista telematico

Sommario: Premessa - 15.1. Controllare la validità dei certificati di Firma Digitale – 15.2. Controllare la scadenza del servizio di Posta Elettronica Certificata – 15.3. Segnalare l'eventuale variazione dell'indirizzo di Posta Elettronica Certificata. – 15.4. Controllare la capienza della posta elettronica certificata – 15.5. Effettuare la manutenzione della casella di Posta Elettronica Certificata. – 15.6. Effettuare settimanalmente il backup. – 15.7. Controllare la presenza di eventuali avvisi sul Portale dei Servizi Telematici del Ministero della Giustizia.

Premessa.
L'esperienza maturata mi porta a suggerire, soprattutto a coloro che non hanno mai avuto un buon rapporto con il mezzo informatico, alcuni consigli attraverso i quali sarà possibile evitare il verificarsi di situazioni critiche che potrebbero avere riflessi negativi nell'esercizio dell'attività professionale.
Per tale motivo consiglio al professionista telematico di non dimenticare mai di …

15.1 - Controllare la validità dei certificati di Firma Digitale.
All'interno del dispositivo di firma digitale risiedono due certificati:
- il certificato di identificazione;
- il certificato di sottoscrizione;

Il primo è quello che, ad es., ci consente di utilizzare il Polisweb mentre il secondo è quello che consente di apporre la firma digitale in un documento informatico (file).
Tali certificati hanno validità limitata; conseguentemente il professionista dovrà curare il rinnovo degli stessi prima della loro scadenza in quanto, i certificati già scaduti non sono rinnovabili cosa questa che comporterebbe l'acquisto di un nuovo dispositivo di firma digitale con costi di gran lunga superiori a quelli del semplice rinnovo dei certificati oltre a non consentire, fino al rilascio del nuovo dispositivo, la possibilità di accedere al Polisweb e di firmare digitalmente i propri atti.
La verifica della validità dei certificati presenti nella Smart Card o Business Key è effettuabile utilizzando la funzione solitamente messa a disposizione dal software rilasciato dalla società dalla quale il dispositivo è stato acquistato; con tale funzione è possibile conoscere la data di inizio e fine validità dei certificati.
Verificate quindi le date di scadenza dei certificati e rinnovate gli stessi prima della loro scadenza.

15.2 - Controllare la scadenza del servizio di Posta Elettronica Certificata.
Anche il servizio di posta elettronica certificata è soggetto a scadenza per cui l'avvocato dovrà avere cura di rinnovare tempestivamente l'erogazione di tale servizio; caso contrario non potrà ricevere e inviare comunicazioni tramite la PEC.

15.3 - Segnalare l'eventuale variazione dell'indirizzo di Posta Elettronica Certificata.
Ove l'avvocato cambi il proprio indirizzo di posta elettronica certificata dovrà avere cura di comunicare immediatamente al proprio Consiglio dell'Ordine tale variazione affinché l'Ordine possa provvedere a comunicare al REGINDE il nuovo indirizzo; ove ciò non avvenga le comunicazioni telematiche dalle cancellerie continueranno a giungere all'indirizzo PEC indicato in precedenza dal professionista.

A tal proposito aggiungo e ricordo che le cancellerie, a prescindere dall'indirizzo di posta elettronica certificata indicato nell'atto depositato, utilizzano per le relative comunicazioni e inoltro di biglietti solo ed esclusivamente quello risultante dal REGINDE.

15.4 - Controllare la capienza della Posta Elettronica Certificata.
la Posta Elettronica Certificata non ha capienza illimitata; raggiunto il limite di capienza la stessa non sarà più in grado di ricevere messaggi. Il verificarsi di ciò non consentirebbe la ricezione della comunicazioni telematiche dalle cancellerie e le stesse, senza ulteriore avviso, sarebbero depositate in cancelleria.

15.5 - Effettuare la manutenzione della casella di Posta Elettronica Certificata.
Ai sensi dell'art. 20 del DM 44/2011 l'avvocato dovrà:
- effettuare la manutenzione ordinaria in quanto sarà il titolare della PEC a rispondere di eventuali malfunzionamenti;
- dotare tutti i terminali informatici, tramite i quali opererà con il PCT, di software idoneo a verificare l'assenza di virus per ogni messaggio in arrivo e in partenza e di software antispam idoneo a prevenire la trasmissione di messaggi di posta elettronica indesiderati;
- conservare "**con ogni mezzo idoneo**" le ricevute di avvenuta consegna dei messaggi trasmessi al dominio giustizia; sul punto evidenzio che il significato della frase "conservare con ogni mezzo idoneo" è riferito alla conservazione digitale di tali ricevute e non anche a quella cartacea in quanto solo la prima potrà provare quanto nella stessa contenuto a meno che non si adotti la procedura prevista dall'art. 23 del codice dell'amministrazione digitale il quale 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"*;
- dotarsi di servizio automatico di avviso dell'imminente saturazione della propria PEC e altresì dovrà verificare la effettiva disponibilità dello spazio disco a disposizione (almeno un giga).

15.6 - Effettuare settimanalmente il backup.
Il codice in materia di protezione dei dati personali[35] prevede che il professionista, a riguardo dei dati sensibili e giudiziari, effettui il backup, dal proprio computer, di tali dati almeno ogni sette giorni solari; ben si comprende come tale obbligo riguardi anche e soprattutto i dati inseriti nei software residenti sul computer al fine di poter depositare telematicamente atti giudiziari.

15.7 – Controllare la presenza di eventuali avvisi sul Portale dei Servizi Telematici del Ministero della Giustizia.
Al fine di non aver brutte sorprese al momento del deposito telematicamente del proprio atto, consiglio al collega di avere cura, anche, di controllare periodicamente, il Portale dei Servizi Telematici del Ministero della Giustizia[36]; in tale portale, solitamente con alcuni giorni di anticipo, vengono inseriti avvisi relativi a:
problemi e/o disservizi di consultazione dei sistemi informatici che consentono il collegamento con le cancellerie degli uffici giudiziari;
impossibilità di effettuare i pagamenti telematici;

[35] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248
[36] http://pst.giustizia.it/PST/it/homepage.wp

impossibilità di effettuare i depositi telematici;
impossibilità di consultare il REGINDE.
Analoghi messaggi vengono solitamente inseriti anche nei PDA privati.
Per meglio rendere l'idea, trascrivo l'avviso apparso sul Portale dei Servizi Telematici il giorno 4 ottobre 2013:

Interruzione servizi Portale dei Servizi Telematici 18/10/2013[37]
04/10/13
Si comunica che a causa di improrogabili interventi di manutenzione, il sito web del Portale dei Servizi Telematici non sarà disponibile in data 18 ottobre 2013, dalle ore 14 alle ore 18 circa. Si precisa che saranno indisponibili i servizi di consultazione registri e pagamenti telematici. Inoltre, saranno indisponibili i servizi di registrazione e consultazione del Registro Generale degli Indirizzi Elettronici (ReGIndE).
Tali servizi saranno indisponibili anche attraverso i Punti di Accesso o software specifici.

Sarà opportuno che il collega, ove il disservizio riguardi in particolare le funzionalità del deposito telematico, eviti di depositare telematicamente il proprio atto fino al ripristino delle funzionalità, anticipando o posticipando il deposito dello stesso.

[37] http://pst.giustizia.it/PST/it/pst_3_1.wp?previousPage=pst_3&contentId=NEW813

Capitolo XVI
La normativa vigente del processo telematico

Sommario: 16.1. Il Codice dell'Amministrazione Digitale - 16.2. Il D.M. 21 febbraio 2011, n. 44 – 16.3 Le specifiche tecniche del 18 luglio 2011 – 16.4 Legge 21 gennaio 1994 n. 53 (facoltà di notificazioni di atti civili, amministrativi e stragiudiziali per gli avvocati.

16.1 - Codice dell'Amministrazione Digitale

CODICE DELL'AMMINISTRAZIONE DIGITALE

Decreto Legislativo 7 marzo 2005, n. 82

Testo vigente dal 21/08/2013[38]

Avvertenza: Testo redatto al solo fine di facilitare la lettura del Codice dell'amministrazione digitale a seguito della modifica introdotta, da ultimo, dal decreto legge 21 giugno 2013 n. 69, convertito con modificazioni dalla L. 9 agosto 2013, n. 98.

Si precisa che il testo normativo qui di seguito esposto (così come quello di qualsiasi altra disposizione normativa pubblicata sul sito dell'Agenzia) non ha alcun carattere di ufficialità: l'unico testo ufficiale e definitivo è quello pubblicato sulla Gazzetta Ufficiale Italiana a mezzo stampa, che prevale in casi di discordanza. L'Agenzia per l'Italia Digitale non è responsabile di eventuali errori o imprecisioni, nonché di danni conseguenti ad azioni o determinazioni assunte in base alla consultazione del testi di legge riportati.

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76, 87 e 117, secondo comma, lettera r), della Costituzione;
Visto l'articolo 14 della legge 23 agosto 1988, n. 400 , recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri;
Visto l'articolo 10 della legge 29 luglio 2003, n. 229 , recante interventi in materia di qualità della regolazione, riassetto normativo e codificazione - legge di semplificazione 2001;
Vista la legge 7 agosto 1990, n. 241 , recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
Visto il decreto legislativo 12 febbraio 1993, n. 39 , recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'articolo 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421;
Visto il decreto legislativo 30 luglio 1999, n. 300 , recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri;

[38] http://www.digitpa.gov.it/amministrazione-digitale/CAD-testo-vigente

Visto il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Testo A), di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 ;
Visto il decreto legislativo 30 marzo 2001, n. 165 , recante norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;
Visto il decreto legislativo 23 gennaio 2002, n. 10 , recante attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche;
Visto il decreto legislativo 30 giugno 2003, n. 196 , recante codice in materia di protezione dei dati personali;
Vista la legge 9 gennaio 2004, n. 4 , recante disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici;
Visto il decreto legislativo 20 febbraio 2004, n. 52 , recante attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA;
Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione dell'11 novembre 2004;
Esperita la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del 22 giugno 1998 del Parlamento europeo e del Consiglio, modificata dalla direttiva 98/48/CE del 20 luglio 1998 del Parlamento europeo e del Consiglio, attuata dalla legge 21 giugno 1986, n. 317 , così come modificata dal decreto legislativo 23 novembre 2000, n. 427 ;
Acquisito il parere della Conferenza unificata, ai sensi dell'articolo 8, del decreto legislativo 28 agosto 1997, n. 281 , espresso nella riunione del 13 gennaio 2005;
Sentito il Garante per la protezione dei dati personali;
Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 7 febbraio 2005;
Acquisito il parere delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;
Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 4 marzo 2005;
Sulla proposta del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, con il Ministro dell'economia e delle finanze, con il Ministro dell'interno, con il Ministro della giustizia, con il Ministro delle attività produttive e con il Ministro delle comunicazioni;

Emana il seguente decreto legislativo:

Capo I
Principi generali
Sezione I
Definizioni, finalità e àmbito di applicazione

Articolo 1.
Definizioni.

1. Ai fini del presente codice si intende per:
a) allineamento dei dati: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;
b) autenticazione del documento informatico: la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione; (1)

c) carta d'identità elettronica: il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare; (2)
d) carta nazionale dei servizi: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;
e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche; (3)
f) 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;
g) certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;
h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;
i) 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;
i-bis) copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto; (4)
i-ter) copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto; (5)
i-quater) copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari; (6)
i-quinquies) duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario; (7)
l) dato a conoscibilità limitata: il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;
m) dato delle pubbliche amministrazioni: il dato formato, o comunque trattato da una pubblica amministrazione;
n) dato pubblico: il dato conoscibile da chiunque;
n-bis) Riutilizzo: uso del dato di cui all'articolo 2, comma 1, lettera e), del decreto legislativo 24 gennaio 2006, n. 36; (236)
o) disponibilità: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge;
p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;
p-bis) documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti; (8)
q) 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; (9)
q-bis) 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; (10)

r) 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; (11)
s) 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; (12)
t) fruibilità di un dato: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;
u) gestione informatica dei documenti: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'àmbito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;
u-bis) gestore di posta elettronica certificata: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata; (13)
u-ter) identificazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso; (14)
v) originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;
v-bis) 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; (15)
z) 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; (16)
aa) titolare: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;
bb) 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.

Articolo 2.

Finalità e àmbito di applicazione.

1. Lo Stato, le regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.
2. Le disposizioni del presente codice si applicano alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 , nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione , nonché alle 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) ai sensi dell'articolo 1, comma 5, della legge 30 dicembre 2004, n. 311. (17)
2-bis. Abrogato. (18)
3. Le disposizioni di cui al capo II, agli articoli 40, 43 e 44 del capo III, nonché al capo IV, si applicano ai privati ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 , e successive modificazioni. (19)
4. Le disposizioni di cui al capo V, concernenti l'accesso ai documenti informatici, e la fruibilità delle informazioni digitali si applicano anche ai gestori di servizi pubblici ed agli organismi di diritto pubblico.
5. Le disposizioni del presente codice si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196 . I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato. (20)
6. Le disposizioni del presente codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, e consultazioni elettorali. Con decreti del Presidente del Consiglio dei Ministri, tenuto conto delle esigenze derivanti dalla natura delle proprie particolari funzioni, sono stabiliti le modalità, i limiti ed i tempi di applicazione delle disposizioni del presente Codice alla Presidenza del Consiglio dei Ministri, nonché all'Amministrazione economico-finanziaria. (21)

Sezione II
Diritti dei cittadini e delle imprese

Articolo 3.
Diritto all'uso delle tecnologie.

1. I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni, con i soggetti di cui all' articolo 2, comma 2, e con i gestori di pubblici servizi ai sensi di quanto previsto dal presente codice. (22)
1-bis. Abrogato. (23)
1-ter. La tutela giurisdizionale davanti al giudice amministrativo è disciplinata dal codice del processo amministrativo. (24)

Articolo 3-bis.
Domicilio digitale del cittadino.

1. Al fine di facilitare la comunicazione tra pubbliche amministrazioni e cittadini, è facoltà di ogni cittadino indicare alla pubblica amministrazione, secondo le modalità stabilite al comma 3, un proprio indirizzo di posta elettronica certificata, rilasciato ai sensi dell'articolo 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2 quale suo domicilio digitale.
2. L'indirizzo di cui al comma 1 è inserito nell'Anagrafe nazionale della popolazione residente-ANPR e reso disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi.
3. Con decreto del Ministro dell'interno, di concerto con il Ministro per la pubblica amministrazione e la semplificazione e il Ministro delegato per l'innovazione tecnologica, sentita

l'Agenzia per l'Italia digitale, sono 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.
4. 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.
4.-bis In assenza del domicilio digitale di cui al comma 1, le amministrazioni possono predisporre le comunicazioni ai cittadini 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 sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del decreto legislativo 12 dicembre 1993, n. 39.
4.-ter Le disposizioni di cui al comma 4-bis 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 di cui all'articolo 71.
4.-quater . Le modalità di predisposizione della copia analogica di cui ai commi 4-bis e 4-ter soddisfano le condizioni di cui all'articolo 23-ter, comma 5, salvo i casi in cui il documento rappresenti, per propria natura, una certificazione rilasciata dall'amministrazione da utilizzarsi nei rapporti tra privati.
5.Dall'attuazione delle disposizioni di cui al presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. (248)

Articolo 4.
Partecipazione al procedimento amministrativo informatico.

1. La partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l'uso delle tecnologie dell'informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 .
2. Ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie dell'informazione e della comunicazione se formato ed inviato nel rispetto della vigente normativa.

Articolo 5.
Effettuazione di pagamenti con modalità informatiche.

1.I soggetti di cui all'articolo 2, comma 2, e i gestori di pubblici servizi nei rapporti con l'utenza sono tenuti a far data dal 1° giugno 2013 ad accettare i pagamenti ad essi spettanti, a qualsiasi titolo dovuti, anche con l'uso delle tecnologie dell'informazione e della comunicazione. A tal fine:
*a)*sono tenuti a pubblicare nei propri siti istituzionali e a specificare nelle richieste di pagamento:
*1)*i codici IBAN identificativi del conto di pagamento, ovvero dell'imputazione del versamento in Tesoreria, di cui all'articolo 3 del decreto del Ministro dell'economia e delle finanze 9 ottobre

2006, n. 293, tramite i quali i soggetti versanti possono effettuare i pagamenti mediante bonifico bancario o postale, ovvero gli identificativi del conto corrente postale sul quale i soggetti versanti possono effettuare i pagamenti mediante bollettino postale;
*2)*i codici identificativi del pagamento da indicare obbligatoriamente per il versamento;
b) si avvalgono di prestatori di servizi di pagamento, individuati mediante ricorso agli strumenti di acquisto e negoziazione messi a disposizione da Consip o dalle centrali di committenza regionali di riferimento costituite ai sensi dell'articolo 1, comma 455, della legge 27 dicembre 2006, n. 296, per consentire ai privati di effettuare i pagamenti in loro favore attraverso l'utilizzo di carte di debito, di credito, prepagate ovvero di altri strumenti di pagamento elettronico disponibili, che consentano anche l'addebito in conto corrente, indicando sempre le condizioni, anche economiche, per il loro utilizzo. Il prestatore dei servizi di pagamento, che riceve l'importo dell'operazione di pagamento, effettua il riversamento dell'importo trasferito al tesoriere dell'ente, registrando in apposito sistema informatico, a disposizione dell'amministrazione, il pagamento eseguito, i codici identificativi del pagamento medesimo, nonché i codici IBAN identificativi dell'utenza bancaria ovvero dell'imputazione del versamento in Tesoreria. Le modalità di movimentazione tra le sezioni di Tesoreria e Poste Italiane S.p.A. dei fondi connessi alle operazioni effettuate sui conti correnti postali intestati a pubbliche amministrazioni sono regolate dalla convenzione tra il Ministero dell'economia e delle finanze e Poste Italiane S.p.A. stipulata ai sensi dell'articolo 2, comma 2, del decreto-legge 1° dicembre 1993, n. 487, convertito, con modificazioni, dalla legge 29 gennaio 1994, n. 71.
2. Per le finalità di cui al comma 1, lettera b), le amministrazioni e i soggetti di cui al comma 1 possono altresì avvalersi dei servizi erogati dalla piattaforma di cui all'articolo 81 comma 2-bis e dei prestatori di servizi di pagamento abilitati.
3. Dalle previsioni di cui al comma 1 sono escluse le operazioni di competenza delle Agenzie fiscali, ai sensi degli articoli 62 e 63 del decreto legislativo 30 luglio 1999, n. 300, nonché delle entrate riscosse a mezzo ruolo. Dalle previsioni di cui alla lettera a) del comma 1 possono essere escluse le operazioni di pagamento per le quali la verifica del buon fine dello stesso debba essere contestuale all'erogazione del servizio; in questi casi devono comunque essere rese disponibili modalità di pagamento di cui alla lettera b) del medesimo comma 1.
3-bis.I micro-pagamenti dovuti a titolo di corrispettivo dalle pubbliche amministrazioni di cui all'articolo 1, comma 450, della legge 27 dicembre 2006, n. 296, come modificato dall'articolo 7, comma 2, del decreto-legge 7 maggio 2012, n. 52, convertito, con modificazioni, dalla legge 6 luglio 2012, n. 94, per i contratti di acquisto di beni e servizi conclusi tramite gli strumenti elettronici di cui al medesimo articolo 1, comma 450, stipulati nelle forme di cui all'articolo 11, comma 13, del codice di cui al decreto legislativo 12 aprile 2006, n. 163, e successive modificazioni, sono effettuati mediante strumenti elettronici di pagamento se richiesto dalle imprese fornitrici.
3-ter.Con decreto del Ministero dell'economia e delle finanze da pubblicare entro il 1° marzo 2013 sono definiti i micro-pagamenti in relazione al volume complessivo del contratto e sono adeguate alle finalità di cui al comma 3-bis le norme relative alle procedure di pagamento delle pubbliche amministrazioni di cui al citato articolo 1, comma 450, della legge n. 296 del 2006. Le medesime pubbliche amministrazioni provvedono ad adeguare le proprie norme al fine di consentire il pagamento elettronico per gli acquisti di cui al comma 3-bis entro il 1° gennaio 2013
4. L'Agenzia per l'Italia digitale, sentita la Banca d'Italia, definisce linee guida per la specifica dei codici identificativi del pagamento di cui al comma 1, lettere a) e b) e le modalità attraverso le quali il prestatore dei servizi di pagamento mette a disposizione dell'ente le informazioni relative al pagamento medesimo.

5. Le attività previste dal presente articolo si svolgono con le risorse umane, finanziarie e strumentali disponibili a legislazione vigente.(25).

Articolo 5-bis.
Comunicazioni tra imprese e amministrazioni pubbliche.

1. La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.
2. Con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro per la pubblica amministrazione e l'innovazione, di concerto con il Ministro dello sviluppo economico e con il Ministro per la semplificazione normativa, sono adottate le modalità di attuazione del comma 1 da parte delle pubbliche amministrazioni centrali e fissati i relativi termini.
3. DigitPA, anche avvalendosi degli uffici di cui all' articolo 17, provvede alla verifica dell'attuazione del comma 1 secondo le modalità e i termini indicati nel decreto di cui al comma 2 .
4. Il Governo promuove l'intesa con regioni ed enti locali in sede di Conferenza unificata per l'adozione degli indirizzi utili alla realizzazione delle finalità di cui al comma 1 (26).

Articolo 6.
Utilizzo della posta elettronica certificata.

1. Per le comunicazioni di cui all' articolo 48, comma 1 , con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano 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 (27).
1-bis. La consultazione degli indirizzi di posta elettronica certificata, di cui agli articoli 16, comma 10, e 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185 , convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2 , e l'estrazione di elenchi dei suddetti indirizzi, da parte delle pubbliche amministrazioni è effettuata sulla base delle regole tecniche emanate da DigitPA, sentito il Garante per la protezione dei dati personali (28).
2. Abrogato (29).
2-bis. Abrogato (30 .

Articolo 6-bis.
Indice nazionale degli indirizzi PEC delle imprese e dei professionisti.

1. Al fine di favorire 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, è istituito, entro sei mesi dalla data di entrata in vigore della presente disposizione e con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, il pubblico elenco denominato Indice nazionale degli indirizzi di posta elettronica certificata (INI-PEC) delle imprese e dei professionisti, presso il Ministero per lo sviluppo economico.
2. L'Indice nazionale di cui al comma 1 è realizzato a partire dagli elenchi di indirizzi PEC costituiti presso il registro delle imprese e gli ordini o collegi professionali, in attuazione di quanto previsto dall'articolo 16 del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2.

3. L'accesso all'INI-PEC è 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, secondo la definizione di cui all'articolo 68, comma 3.
4. Il Ministero per lo sviluppo economico, 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 di cui al comma 1 delle strutture informatiche delle Camere di commercio deputate alla gestione del registro imprese e ne definisce con proprio decreto, da emanare entro 60 giorni dalla data di entrata in vigore della presente disposizione, le modalità di accesso e di aggiornamento.
5. Nel decreto di cui al comma 4 sono anche definite le modalità e le forme con cui gli ordini e i collegi professionali comunicano all'Indice nazionale di cui al comma 1 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.
6. Dall'attuazione delle disposizioni di cui al presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. (249)

Articolo 7.
Qualità dei servizi resi e soddisfazione dell'utenza.

1. Le pubbliche amministrazioni provvedono alla riorganizzazione ed aggiornamento dei servizi resi; a tale fine sviluppano l'uso delle tecnologie dell'informazione e della comunicazione, sulla base di una preventiva analisi delle reali esigenze dei cittadini e delle imprese, anche utilizzando strumenti per la valutazione del grado di soddisfazione degli utenti (31).
2. Entro il 31 maggio di ciascun anno le pubbliche amministrazioni centrali trasmettono al Ministro delegato per la funzione pubblica e al Ministro delegato per l'innovazione e le tecnologie una relazione sulla qualità dei servizi resi e sulla soddisfazione dell'utenza.

Articolo 8.
Alfabetizzazione informatica dei cittadini.

1. Lo Stato promuove iniziative volte a favorire l'alfabetizzazione informatica dei cittadini con particolare riguardo alle categorie a rischio di esclusione, anche al fine di favorire l'utilizzo dei servizi telematici delle pubbliche amministrazioni.

Articolo 9.
Partecipazione democratica elettronica.

1. Le pubbliche amministrazioni favoriscono ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi (32).

Articolo 10.
Sportello unico per le attività produttive (33).

1. Lo sportello unico per le attività produttive di cui all'articolo 38, comma 3, del decreto-legge 25 giugno 2008, n. 112 , convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133 , eroga i propri servizi verso l'utenza in via telematica (34).
2. Abrogato (35).
3. Abrogato (36).
4. Lo Stato realizza, nell'àmbito di quanto previsto dal sistema pubblico di connettività di cui al presente decreto, un sistema informatizzato per le imprese relativo ai procedimenti di competenza delle amministrazioni centrali anche ai fini di quanto previsto all' articolo 11 (37).

Articolo 11.
Registro informatico degli adempimenti amministrativi per le imprese.

1. Presso il Ministero delle attività produttive, che si avvale a questo scopo del sistema informativo delle camere di commercio, industria, artigianato e agricoltura, è istituito il Registro informatico degli adempimenti amministrativi per le imprese, di seguito denominato «Registro», il quale contiene l'elenco completo degli adempimenti amministrativi previsti dalle pubbliche amministrazioni per l'avvio e l'esercizio delle attività di impresa, nonché i dati raccolti dalle amministrazioni comunali negli archivi informatici di cui all'articolo 24, comma 2, del decreto legislativo 31 marzo 1998, n. 112 . Il Registro, che si articola su base regionale con apposite sezioni del sito informatico, fornisce, ove possibile, il supporto necessario a compilare in via elettronica la relativa modulistica.
2. È fatto obbligo alle amministrazioni pubbliche, nonché ai concessionari di lavori e ai concessionari e gestori di servizi pubblici, di trasmettere in via informatica al Ministero delle attività produttive l'elenco degli adempimenti amministrativi necessari per l'avvio e l'esercizio dell'attività di impresa.
3. Con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro delle attività produttive e del Ministro delegato per l'innovazione e le tecnologie, sono stabilite le modalità di coordinamento, di attuazione e di accesso al Registro, nonché di connessione informatica tra le diverse sezioni del sito (38).
4. Il Registro è pubblicato su uno o più siti telematici, individuati con decreto del Ministro delle attività produttive.
5. Del Registro possono avvalersi le autonomie locali, qualora non provvedano in proprio, per i servizi pubblici da loro gestiti.
6. All'onere derivante dall'attuazione del presente articolo si provvede ai sensi dell'articolo 21, comma 2, della legge 29 luglio 2003, n. 229 .

Sezione III
Organizzazione delle pubbliche amministrazioni rapporti fra Stato, regioni e autonomie locali

Articolo 12.
Norme generali per l'uso delle tecnologie dell'informazione e delle comunicazioni nell'azione amministrativa.

1. Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, (242) nonché per la garanzia dei diritti dei cittadini e delle imprese di cui al capo I, sezione II , del presente decreto (39).

1-bis. Gli organi di Governo nell'esercizio delle funzioni di indirizzo politico ed in particolare nell'emanazione delle direttive generali per l'attività amministrativa e per la gestione ai sensi del comma 1 dell'articolo 14 del decreto legislativo 30 marzo 2001, n. 165 , e le amministrazioni pubbliche nella redazione del piano di performance di cui all'articolo 10 del decreto legislativo 27 ottobre 2009, n. 150 , dettano disposizioni per l'attuazione delle disposizioni del presente decreto (40).
1-ter. I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al presente decreto ai sensi e nei limiti degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165 , ferme restando le eventuali responsabilità penali, civili e contabili previste dalle norme vigenti. L'attuazione delle disposizioni del presente decreto è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti (41).
2. Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche, e procedurali di sicurezza, secondo le regole tecniche di cui all' articolo 71.
3. Le pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici, ivi comprese le reti di telefonia fissa e mobile in tutte le loro articolazioni, da esse erogati, qualunque sia il canale di erogazione, nel rispetto della autonomia e della specificità di ciascun erogatore di servizi (42).
4. Lo Stato promuove la realizzazione e l'utilizzo di reti telematiche come strumento di interazione tra le pubbliche amministrazioni ed i privati.
5. Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche stabilite ai sensi dell' articolo 71.
5-bis. Le pubbliche amministrazioni implementano e consolidano i processi di informatizzazione in atto, ivi compresi quelli riguardanti l'erogazione attraverso le tecnologie dell'informazione e della comunicazione in via telematica di servizi a cittadini ed imprese anche con l'intervento di privati (43).

Articolo 13.
Formazione informatica dei dipendenti pubblici.

1. Le pubbliche amministrazioni nella predisposizione dei piani di cui all'articolo 7-bis, del decreto legislativo 30 marzo 2001, n. 165 , e nell'àmbito delle risorse finanziarie previste dai piani medesimi, attuano anche politiche di formazione del personale finalizzate alla conoscenza e all'uso delle tecnologie dell'informazione e della comunicazione, nonché dei temi relativi all'accessibilità e alle tecnologie assistite, ai sensi dell'articolo 8 della legge 9 gennaio 2004, n. 4. (234)

Articolo 14.
Rapporti tra Stato, regioni e autonomie locali.

1. In attuazione del disposto dell'articolo 117, secondo comma, lettera r), della Costituzione , lo Stato disciplina il coordinamento informatico dei dati dell'amministrazione statale, regionale e locale, dettando anche le regole tecniche necessarie per garantire la sicurezza e l'interoperabilità dei sistemi informatici e dei flussi informativi per la circolazione e lo scambio dei dati e per l'accesso ai servizi erogati in rete dalle amministrazioni medesime.

2. Lo Stato, le regioni e le autonomie locali promuovono le intese e gli accordi e adottano, attraverso la Conferenza unificata, gli indirizzi utili per realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso e per l'individuazione delle regole tecniche di cui all' articolo 71.
2-bis. Le regioni promuovono sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali (44).
2-ter. Le regioni e gli enti locali digitalizzano la loro azione amministrativa e implementano l'utilizzo delle tecnologie dell'informazione e della comunicazione per garantire servizi migliori ai cittadini e alle imprese (45).
3. Lo Stato, ai fini di quanto previsto ai commi 1 e 2 , istituisce organismi di cooperazione con le regioni e le autonomie locali, promuove intese ed accordi tematici e territoriali, favorisce la collaborazione interregionale, incentiva la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle soluzioni tecniche ed organizzative, previene il divario tecnologico tra amministrazioni di diversa dimensione e collocazione territoriale.
3-bis. Ai fini di quanto previsto ai commi 1 , 2 e 3 , è istituita senza nuovi o maggiori oneri per la finanza pubblica, presso la Conferenza unificata, previa delibera della medesima che ne definisce la composizione e le specifiche competenze, una Commissione permanente per l'innovazione tecnologica nelle regioni e negli enti locali con funzioni istruttorie e consultive (46).

Articolo 15.
Digitalizzazione e riorganizzazione.

1. La riorganizzazione strutturale e gestionale delle pubbliche amministrazioni volta al perseguimento degli obiettivi di cui all' articolo 12, comma 1, avviene anche attraverso il migliore e più esteso utilizzo delle tecnologie dell'informazione e della comunicazione nell'àmbito di una coordinata strategia che garantisca il coerente sviluppo del processo di digitalizzazione.
2. In attuazione del comma 1, le pubbliche amministrazioni provvedono in particolare a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese, assicurando che l'utilizzo delle tecnologie dell'informazione e della comunicazione avvenga in conformità alle prescrizioni tecnologiche definite nelle regole tecniche di cui all' articolo 71.
2-bis. Le pubbliche amministrazioni nella valutazione dei progetti di investimento in materia di innovazione tecnologica tengono conto degli effettivi risparmi derivanti dalla razionalizzazione di cui al comma 2, nonché dei costi e delle economie che ne derivano (47).
2-ter. Le pubbliche amministrazioni, quantificano annualmente, ai sensi dell'articolo 27, del decreto legislativo 27 ottobre 2009, n. 150 , i risparmi effettivamente conseguiti in attuazione delle disposizioni di cui ai commi 1 e 2. Tali risparmi sono utilizzati, per due terzi secondo quanto previsto dall'articolo 27, comma 1, del citato decreto legislativo n. 150 del 2009 e in misura pari ad un terzo per il finanziamento di ulteriori progetti di innovazione (48).
3. La digitalizzazione dell'azione amministrativa è attuata dalle pubbliche amministrazioni con modalità idonee a garantire la partecipazione dell'Italia alla costruzione di reti trans europee per lo scambio elettronico di dati e servizi fra le amministrazioni dei Paesi membri dell'Unione europea (49).

Articolo 16.
Competenze del Presidente del Consiglio dei Ministri in materia di innovazione e tecnologie.

1. Per il perseguimento dei fini di cui al presente codice, il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie, nell'attività di coordinamento del processo di digitalizzazione e di coordinamento e di valutazione dei programmi, dei progetti e dei piani di azione formulati dalle pubbliche amministrazioni centrali per lo sviluppo dei sistemi informativi:
a) definisce con proprie direttive le linee strategiche, la pianificazione e le aree di intervento dell'innovazione tecnologica nelle pubbliche amministrazioni centrali, e ne verifica l'attuazione;
b) valuta, sulla base di criteri e metodiche di ottimizzazione della spesa, il corretto utilizzo delle risorse finanziarie per l'informatica e la telematica da parte delle singole amministrazioni centrali;
c) sostiene progetti di grande contenuto innovativo, di rilevanza strategica, di preminente interesse nazionale, con particolare attenzione per i progetti di carattere intersettoriale;
d) promuove l'informazione circa le iniziative per la diffusione delle nuove tecnologie;
e) detta norme tecniche ai sensi dell' articolo 71 e criteri in tema di pianificazione, progettazione, realizzazione, gestione, mantenimento dei sistemi informativi automatizzati delle pubbliche amministrazioni centrali e delle loro interconnessioni, nonché della loro qualità e relativi aspetti organizzativi e della loro sicurezza.
2. Il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie riferisce annualmente al Parlamento sullo stato di attuazione del presente codice.

Articolo 17.
Strutture per l'organizzazione, l'innovazione e le tecnologie.

1. Le pubbliche amministrazioni centrali garantiscono l'attuazione delle linee strategiche per la riorganizzazione e digitalizzazione dell'amministrazione definite dal Governo. A tale fine, le predette amministrazioni individuano un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, responsabile del coordinamento funzionale. Al predetto ufficio afferiscono i compiti relativi a (50):
a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni (51);
b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione (52);
c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1 (53);
d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
e) analisi della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
*f)*cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia (54);
h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j) 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 (55).
1-bis. Per lo svolgimento dei compiti di cui al comma 1, le Agenzie, le Forze armate, compresa l'Arma dei carabinieri e il Corpo delle capitanerie di porto, nonché i Corpi di polizia hanno facoltà di individuare propri uffici senza incrementare il numero complessivo di quelli già previsti nei rispettivi assetti organizzativi. (56)
1-ter. DigitPA assicura il coordinamento delle iniziative di cui al comma 1, lettera c), con le modalità di cui all' articolo 51. (57)

Articolo 18.
Conferenza permanente per l'innovazione tecnologica.

1. È istituita la Conferenza permanente per l'innovazione tecnologica con funzioni di consulenza al Presidente del Consiglio dei Ministri, o al Ministro delegato per l'innovazione e le tecnologie, in materia di sviluppo ed attuazione dell'innovazione tecnologica nelle amministrazioni dello Stato.
2. La Conferenza permanente per l'innovazione tecnologica è presieduta da un rappresentante della Presidenza del Consiglio dei Ministri designato dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie; ne fanno parte il Presidente del DigitPA, (d'ora in poi DigitPA), i componenti del DigitPA, il Capo del Dipartimento per l'innovazione e le tecnologie, nonché i responsabili delle funzioni di cui all' articolo 17 (58).
3. La Conferenza permanente per l'innovazione tecnologica si riunisce con cadenza almeno semestrale per la verifica dello stato di attuazione dei programmi in materia di innovazione tecnologica e del piano triennale di cui all'articolo 9 del decreto legislativo 12 febbraio 1993, n. 39.
4. Il Presidente del Consiglio dei Ministri, o il Ministro delegato per l'innovazione e le tecnologie, provvede, con proprio decreto, a disciplinare il funzionamento della Conferenza permanente per l'innovazione tecnologica.
5. La Conferenza permanente per l'innovazione tecnologica può sentire le organizzazioni produttive e di categoria.
6. La Conferenza permanente per l'innovazione tecnologica opera senza rimborsi spese o compensi per i partecipanti a qualsiasi titolo dovuti, compreso il trattamento economico di missione; dal presente articolo non devono derivare nuovi o maggiori oneri per il bilancio dello Stato.

Articolo 19.
Banca dati per la legislazione in materia di pubblico impiego.

1. È istituita presso la Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, una banca dati contenente la normativa generale e speciale in materia di rapporto di lavoro alle dipendenze delle pubbliche amministrazioni.
2. La Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, cura l'aggiornamento periodico della banca dati di cui al comma 1, tenendo conto delle innovazioni normative e della contrattazione collettiva successivamente intervenuta, e assicurando agli utenti la consultazione gratuita.
3. All'onere derivante dall'attuazione del presente articolo si provvede ai sensi dell'articolo 21, comma 3, della legge 29 luglio 2003, n. 229.

Capo II

Documento informatico e firme elettroniche; Trasferimenti di fondi, libri e scritture (59)

Sezione I
Documento informatico

Articolo 20.
Documento informatico.

1. Il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all' articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice. (60)
1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall' articolo 21. (61)
2. Abrogato. (62)
3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, sono stabilite ai sensi dell'articolo 71. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale. (63)
4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.
5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.
5-bis. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell' articolo 71. (64)

Articolo 21.
Documento informatico sottoscritto con firma elettronica. (65)

1. 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. (66)
2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3 , che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile . L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria. (67)
2-bis. Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile , se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale. (68)
3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a

mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.
4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:
a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del 13 dicembre 1999 del Parlamento europeo e del Consiglio, ed è accreditato in uno Stato membro;
b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;
c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.
5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

Articolo 22. (69)
Copie informatiche di documenti analogici.

1. I documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata. La loro esibizione e produzione sostituisce quella dell'originale.
2. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, 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.
3. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all' articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.
4. Le copie formate ai sensi dei commi 1, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.
5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.
6. Fino alla data di emanazione del decreto di cui al comma 5 per tutti i documenti analogici originali unici permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

Articolo 23. (70)
Copie analogiche di documenti informatici.

1. 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.
2. 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 .

Articolo 23-bis. (71)
Duplicati e copie informatiche di documenti informatici.

1. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche di cui all' articolo 71.
2. Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all' articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte 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 .

Articolo 23-ter. (72)
Documenti amministrativi informatici.

1. Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.
2. I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile .
3. Le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico.
4. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il Ministro per i beni e le attività culturali, nonché d'intesa con la Conferenza unificata di cui all'articolo 8 del

decreto legislativo 28 agosto 1997, n. 281 , e sentiti DigitPA e il Garante per la protezione dei dati personali.
5. Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con linee guida dell'Agenzia per l'Italia digitale, tramite il quale è possibile ottenere il documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità.
5-bis. I documenti di cui al presente articolo devono essere fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all'articolo 11 della legge 9 gennaio 2004, n. 4. (235).
6. Per quanto non previsto dal presente articolo si applicano gli articoli 21 , 22 , 23 e 23-bis .

Articolo 23-quater. (73)
Riproduzioni informatiche.

1. All'articolo 2712 del codice civile dopo le parole: « riproduzioni fotografiche » è inserita la seguente: « , informatiche » .

Sezione II
Firme elettroniche e certificatori

Articolo 24.
Firma digitale.

1. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata.
2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.
3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.
4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell' articolo 71 , la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

Articolo 25. (74)
Firma autenticata.

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile , la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.
2. L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

3. L'apposizione della firma digitale da parte del pubblico ufficiale ha l'efficacia di cui all' articolo 24, comma 2.
4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.

Articolo 26.
Certificatori.

1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, qualora emettano certificati qualificati, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385 , e successive modificazioni. (75)
2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.
3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente codice e le relative norme tecniche di cui all' articolo 71 e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE .

Articolo 27.
Certificatori qualificati.

1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall' articolo 26.
2. I certificatori di cui al comma 1, devono inoltre:
a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;
b) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all' articolo 71;
c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;
d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in àmbito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all' articolo 35, comma 5;
e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi.
3. I certificatori di cui al comma 1, devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività al DigitPA, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice. (76)

4. Il DigitPA procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente codice e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa. (77)

Articolo 28.
Certificati qualificati.

1. I certificati qualificati devono contenere almeno le seguenti informazioni:
a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;
b) numero di serie o altro codice identificativo del certificato;
c) nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;
d) nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;
e) dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare;
f) indicazione del termine iniziale e finale del periodo di validità del certificato;
g) firma elettronica del certificatore che ha rilasciato il certificato, realizzata in conformità alle regole tecniche ed idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo. (78)
2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale.
3. Il certificato qualificato può contenere, ove richiesto dal titolare o dal terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto: (79)
a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza; (80)
b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera a) ai sensi dell' articolo 30, comma 3; (81)
c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.
3-bis. Le informazioni di cui al comma 3 possono essere contenute in un separato certificato elettronico e possono essere rese disponibili anche in rete. Con decreto del Presidente del Consiglio dei Ministri sono definite le modalità di attuazione del presente comma, anche in riferimento alle pubbliche amministrazioni e agli ordini professionali. (82)
4. Il titolare, ovvero il terzo interessato se richiedente ai sensi del comma 3, comunicano tempestivamente al certificatore il modificarsi o venir meno delle circostanze oggetto delle informazioni di cui al presente articolo.

Articolo 29.
Accreditamento.

1. I certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono di essere accreditati presso il DigitPA. (83)
2. Il richiedente deve rispondere ai requisiti di cui all' articolo 27, ed allegare alla domanda oltre ai documenti indicati nel medesimo articolo il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole tecniche.
3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2 deve inoltre:
a) avere forma giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385;
b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 del decreto legislativo 1° settembre 1993, n. 385.
4. La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.
5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità del DigitPA o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa. (84)
6. A seguito dell'accoglimento della domanda, il DigitPA dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto dal DigitPA stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione. (85)
7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.
8. Il valore giuridico delle firme elettroniche qualificate e delle firme digitali basate su certificati qualificati rilasciati da certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE è equiparato a quello previsto per le firme elettroniche qualificate e per le firme digitali basate su certificati qualificati emessi dai certificatori accreditati ai sensi del presente articolo. (86)
9. Alle attività previste dal presente articolo si fa fronte nell'àmbito delle risorse del DigitPA, senza nuovi o maggiori oneri per la finanza pubblica. (87)

Articolo 30.
Responsabilità del certificatore.

1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:
a) sull'esattezza e sulla completezza delle informazioni necessarie alla verifica della firma in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;
b) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;

c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi;
d) sull'adempimento degli obblighi a suo carico previsti dall' articolo 32.
2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano affidamento sul certificato stesso, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o non tempestiva sospensione del certificato, secondo quanto previsto. dalle regole tecniche di cui all' articolo 71, salvo che provi d'aver agito senza colpa.
3. Il certificato qualificato può contenere limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel certificato secondo quanto previsto dalle regole tecniche di cui all' articolo 71. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite. (88)

Articolo 31. (89)
Vigilanza sull'attività dei certificatori e dei gestori di posta elettronica certificata.

1. DigitPA svolge funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e dei gestori di posta elettronica certificata.
Articolo 32.
Obblighi del titolare e del certificatore.
1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di forma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma. (90)
2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi. (91)
3. Il certificatore che rilascia, ai sensi dell' articolo 1, certificati qualificati deve inoltre:
a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;
b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all' articolo 71, nel rispetto del decreto legislativo 30 giugno 2003, n. 196 , e successive modificazioni;
c) 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;
d) attenersi alle regole tecniche di cui all' articolo 71;
e) 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;
f) Abrogato; (92)
g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all' articolo 71;

h) 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;
i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari; (93)
k) non copiare, né conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;
l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore;
m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;
m-bis) garantire il corretto funzionamento e la continuità del sistema e comunicare immediatamente a DigitPA e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso. (94)
4. Il certificatore è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.
5. Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

Articolo 32-bis. (95)
Sanzioni per i certificatori qualificati e per i gestori di posta elettronica certificata.

1. Qualora si verifichi, salvi i casi di forza maggiore o caso fortuito, un malfunzionamento nel sistema che determini un disservizio, ovvero la mancata o intempestiva comunicazione dello stesso disservizio a DigitPA o agli utenti, ai sensi dell' articolo 32, comma 3, lettera m-bis), DigitPA diffida il certificatore qualificato o il gestore di posta elettronica certificata a ripristinare la regolarità del servizio o ad effettuare le comunicazioni ivi previste. Se il disservizio ovvero la mancata o intempestiva comunicazione sono reiterati per due volte nel corso di un biennio, successivamente alla seconda diffida si applica la sanzione della cancellazione dall'elenco pubblico.
2. Qualora si verifichi, fatti salvi i casi di forza maggiore o di caso fortuito, un malfunzionamento nel sistema che determini l'interruzione del servizio, ovvero la mancata o intempestiva comunicazione dello stesso disservizio a DigitPA o agli utenti, ai sensi dell' articolo 32, comma 3, lettera m-bis), DigitPA diffida il certificatore qualificato o il gestore di posta elettronica certificata a ripristinare la regolarità del servizio o ad effettuare le comunicazioni ivi previste. Se l'interruzione

del servizio ovvero la mancata o intempestiva comunicazione sono reiterati nel corso di un biennio, successivamente alla prima diffida si applica la sanzione della cancellazione dall'elenco pubblico.
3. Nei casi di cui ai commi 1 e 2 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.
4. Qualora un certificatore qualificato o un gestore di posta elettronica certificata non ottemperi, nei tempi previsti, a quanto prescritto da DigitPA nell'esercizio delle attività di vigilanza di cui all'articolo 31 si applica la disposizione di cui al comma 2.

Articolo 33.
Uso di pseudonimi.

1. In luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale. Se il certificato è qualificato, il certificatore ha l'obbligo di conservare le informazioni relative alla reale identità del titolare per almeno venti anni decorrenti dall'emissione del certificato stesso. (96)

Articolo 34.
Norme particolari per le pubbliche amministrazioni e per altri soggetti qualificati.

1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:
a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell' articolo 29; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto ad esclusione di quelli rilasciati da collegi e ordini professionali e relativi organi agli iscritti nei rispettivi albi e registri; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati; (97)
b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.
2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all' articolo 71. (98)
3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti di cui all' articolo 71 di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei princìpi generali stabiliti dai rispettivi ordinamenti.
4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche vigenti in materia di firme digitali.
5. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni devono dotarsi di idonee procedure informatiche e strumenti software per la verifica delle firme digitali secondo quanto previsto dalle regole tecniche di cui all' articolo 71.

Articolo 35.
Dispositivi sicuri e procedure per la generazione della firma.

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:
a) sia riservata;
b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;
c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.
2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle regole tecniche di cui all' articolo 71.
3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. La firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima. (99)
4. I dispositivi sicuri di firma devono essere dotati di certificazione di sicurezza ai sensi dello schema nazionale di cui al comma 5. (100)
5. La conformità dei requisiti di sicurezza dei dispositivi per la creazione di una firma qualificata prescritti dall'allegato III della direttiva 1999/93/CE è accertata, in Italia, dall'Organismo di certificazione della sicurezza informatica in base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. L'attuazione dello schema nazionale non deve determinare nuovi o maggiori oneri per il bilancio dello Stato. Lo schema nazionale può prevedere altresì la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti afferenti al settore suddetto. La valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma è effettuata dall'Agenzia per l'Italia digitale in conformità ad apposite linee guida da questa emanate, acquisito il parere obbligatorio dell'Organismo di certificazione della sicurezza informatica(101).
6. La conformità di cui al comma 5 è inoltre riconosciuta se accertata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 11, paragrafo 1, lettera b), della direttiva 1999/93/CE . (102)

Articolo 36.
Revoca e sospensione dei certificati qualificati.

1. Il certificato qualificato deve essere a cura del certificatore:
a) revocato in caso di cessazione dell'attività del certificatore salvo quanto previsto dal comma 2 dell'articolo 37; (103)
b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;
c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente codice;
d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.

2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo 71.
3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.
4. Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all' articolo 71.

Articolo 37.
Cessazione dell'attività.

1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso al DigitPA e informare senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati. (104)
2. Il certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. L'indicazione di un certificatore sostitutivo evita la revoca di tutti i certificati non scaduti al momento della cessazione.
3. Il certificatore di cui al comma 1 indica altro depositario del registro dei certificati e della relativa documentazione.
4. Il DigitPA rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all' articolo 29, comma 6. (105)
4-bis. Qualora il certificatore qualificato cessi la propria attività senza indicare, ai sensi del comma 2, un certificatore sostitutivo e non si impegni a garantire la conservazione e la disponibilità della documentazione prevista dagli articoli 33 e 32, comma 3, lettera j) e delle ultime liste di revoca emesse, deve provvedere al deposito presso DigitPA che ne garantisce la conservazione e la disponibilità. (106)

Sezione III
Trasferimenti di fondi, libri e scritture (107)

Articolo 38.
Trasferimenti di fondi. (108)

1. Il trasferimento in via telematica di fondi tra pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo le regole tecniche stabilite ai sensi dell' articolo 71 di concerto con i Ministri per la funzione pubblica, della giustizia e dell'economia e delle finanze, sentiti il Garante per la protezione dei dati personali e la Banca d'Italia.

Articolo 39.
Libri e scritture.

1. I libri, i repertori e le scritture, ivi compresi quelli previsti dalla legge sull'ordinamento del notariato e degli archivi notarili, di cui sia obbligatoria la tenuta possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente codice e secondo le regole tecniche stabilite ai sensi dell' articolo 71.

Capo III
Formazione, gestione e conservazione dei documenti informatici

Articolo 40.
Formazione di documenti informatici.

1. Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all' articolo 71. (109)
2. Abrogato. (110)
3. Con apposito regolamento, da emanarsi entro 180 giorni dalla data di entrata in vigore del presente codice, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400 , sulla proposta dei Ministri delegati per la funzione pubblica, per l'innovazione e le tecnologie e del Ministro per i beni e le attività culturali, sono individuate le categorie di documenti amministrativi che possono essere redatti in originale anche su supporto cartaceo in relazione al particolare valore di testimonianza storica ed archivistica che sono idonei ad assumere.
4. Il Presidente del Consiglio dei Ministri, con propri decreti, fissa la data dalla quale viene riconosciuto il valore legale degli albi, elenchi, pubblici registri ed ogni altra raccolta di dati concernenti stati, qualità personali e fatti già realizzati dalle amministrazioni, su supporto informatico, in luogo dei registri cartacei.

Articolo 40-bis (111)
Protocollo informatico.

1. Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 , le comunicazioni che pervengono o sono inviate dalle caselle di posta elettronica di cui agli articoli 47, commi 1 e 3, 54, comma 2-ter e 57-bis, comma 1, nonché le istanze e le dichiarazioni di cui all' articolo 65 in conformità alle regole tecniche di cui all'articolo 71.

Articolo 41.
Procedimento e fascicolo informatico.

1. Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente.
1-bis. La gestione dei procedimenti amministrativi è attuata in modo da consentire, mediante strumenti automatici, il rispetto di quanto previsto all' articolo 54 , commi 2-ter e 2-quater. (112)
2. La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241. (113)
2-bis. Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento. Le regole per la costituzione, l'identificazione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico ed il sistema pubblico di connettività, e comunque rispettano i criteri dell'interoperabilità e della cooperazione applicativa; regole tecniche specifiche possono essere dettate ai sensi dell' articolo 71, di concerto con il Ministro della funzione pubblica. (114)
2-ter. Il fascicolo informatico reca l'indicazione:

a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
b) delle altre amministrazioni partecipanti;
c) del responsabile del procedimento;
d) dell'oggetto del procedimento;
e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater; (115)
e-bis) dell'identificativo del fascicolo medesimo. (116)
2-quater. Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990. (117)
3. Ai sensi degli articoli da 14 a 14-quinquies della legge 7 agosto 1990, n. 241 , previo accordo tra le amministrazioni coinvolte, la conferenza dei servizi è convocata e svolta avvalendosi degli strumenti informatici disponibili, secondo i tempi e le modalità stabiliti dalle amministrazioni medesime.

Articolo 42.
Dematerializzazione dei documenti delle pubbliche amministrazioni.

1. Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici, nel rispetto delle regole tecniche adottate ai sensi dell' articolo 71.

Articolo 43.
Riproduzione e conservazione dei documenti.

1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell' articolo 71. (118)
2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali.
3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche stabilite ai sensi dell' articolo 71. (119)
4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n. 42 .

Articolo 44.
Requisiti per la conservazione dei documenti informatici.

1. Il sistema di conservazione dei documenti informatici assicura: (120)

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 ;
b) l'integrità del documento;
c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;
d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196 , e dal disciplinare tecnico pubblicato in allegato B a tale decreto.
1-bis. Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196 , e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 , nella definizione e gestione delle attività di rispettiva competenza. (121)
1-ter. Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche. (122)

Articolo 44-bis (123).
Conservatori accreditati.

1. I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono l'accreditamento presso DigitPA.
2. Si applicano, in quanto compatibili, gli articoli 26, 27, 29, ad eccezione del comma 3, lettera a) e 31.
3. I soggetti privati di cui al comma 1 sono costituiti in società di capitali con capitale sociale non inferiore a euro 200.000.

Capo IV
Trasmissione informatica dei documenti

Articolo 45.
Valore giuridico della trasmissione.

1. 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. (124)
2. 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.

Articolo 46.
Dati particolari contenuti nei documenti trasmessi.

1. Al fine di garantire la riservatezza dei dati sensibili o giudiziari di cui all'articolo 4, comma 1 , lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196 , i documenti informatici trasmessi ad altre pubbliche amministrazioni per via telematica possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e indispensabili per il perseguimento delle finalità per le quali sono acquisite.

Articolo 47.
Trasmissione dei documenti attraverso la posta elettronica tra le pubbliche amministrazioni.

1. 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. (125)
1-bis. L'inosservanza della disposizione di cui al comma 1, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare. (243)
2. 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; (126)
c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71. E' in ogni caso esclusa la trasmissione di documenti a mezzo fax; (250)
d) ovvero trasmesse attraverso sistemi di posta elettronica certificata di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
3. Le pubbliche amministrazioni e gli altri soggetti di cui all' articolo 2, comma 2, provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo. 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. (127)

Articolo 48 (128) .
Posta elettronica certificata.

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 , o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA . (129)
2. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.
3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 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, ovvero conformi al decreto del Presidente del Consiglio dei Ministri di cui al comma 1 .

Articolo 49.
Segretezza della corrispondenza trasmessa per via telematica.

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.
2. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Capo V
Dati delle pubbliche amministrazioni e servizi in rete

Sezione I
Dati delle pubbliche amministrazioni

Articolo 50.
Disponibilità dei dati delle pubbliche amministrazioni.

1. I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico.
2. Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all' articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241 , e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo per la prestazione di elaborazioni aggiuntive; è fatto comunque salvo il disposto dell'articolo 43, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 . (130)
3. Al fine di rendere possibile l'utilizzo in via telematica dei dati di una pubblica amministrazione da parte dei sistemi informatici di altre amministrazioni l'amministrazione titolare dei dati predispone, gestisce ed eroga i servizi informatici allo scopo necessari, secondo le regole tecniche del sistema pubblico di connettività di cui al presente decreto. (131)

Articolo 50-bis (132).
Continuità operativa.

1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.
2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono:
a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;
b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.
4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.

Articolo 51.
Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni . (133)

1. Con le regole tecniche adottate ai sensi dell' articolo 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture. (134)
1-bis. DigitPA, ai fini dell'attuazione del comma 1:
a) raccorda le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;
b) promuove intese con le analoghe strutture internazionali;
c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni. (135)
2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.
2-bis. Le amministrazioni hanno l'obbligo di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi. (136)

Articolo 52.
Accesso telematico e riutilizzo dei dati delle pubbliche amministrazioni. (137)

1.L'accesso telematico a dati, documenti e procedimenti e il riutilizzo dei dati e documenti è disciplinato dai soggetti di cui all'articolo 2, comma 2, secondo le disposizioni del presente codice e nel rispetto della normativa vigente. Le pubbliche amministrazioni pubblicano nel proprio sito web, all'interno della sezione "Trasparenza, valutazione e merito", il catalogo dei dati, dei metadati e delle relative banche dati in loro possesso ed i regolamenti che ne disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo, fatti salvi i dati presenti in Anagrafe tributaria.
I dati e i documenti che le amministrazioni titolari pubblicano, con qualsiasi modalità, senza l'espressa adozione di una licenza di cui all'articolo 2, comma 1, lettera h), del decreto legislativo 24 gennaio 2006, n. 36, si intendono rilasciati come dati di tipo aperto ai sensi all'articolo 68,

comma 3, del presente Codice. L'eventuale adozione di una licenza di cui al citato articolo 2, comma 1, lettera h), è motivata ai sensi delle linee guida nazionali di cui al comma 7.
Nella definizione dei capitolati o degli schemi dei contratti di appalto relativi a prodotti e servizi che comportino la raccolta e la gestione di dati pubblici, le pubbliche amministrazioni di cui all'articolo 2, comma 2, prevedono clausole idonee a consentire l'accesso telematico e il riutilizzo, da parte di persone fisiche e giuridiche, di tali dati, dei metadati, degli schemi delle strutture di dati e delle relative banche dati.
Le attività volte a garantire l'accesso telematico e il riutilizzo dei dati delle pubbliche amministrazioni rientrano tra i parametri di valutazione della performance dirigenziale ai sensi dell'articolo 11, comma 9, del decreto legislativo 27 ottobre 2009, n. 150.
L'Agenzia per l'Italia digitale promuove le politiche di valorizzazione del patrimonio informativo pubblico nazionale e attua le disposizioni di cui al capo V del presente Codice.
Entro il mese di febbraio di ogni anno l'Agenzia trasmette al Presidente del Consiglio dei Ministri o al Ministro delegato per l'innovazione tecnologica, che li approva entro il mese successivo, un' Agenda nazionale in cui definisce contenuti e gli obiettivi delle politiche di valorizzazione del patrimonio informativo pubblico e un rapporto annuale sullo stato del processo di valorizzazione in Italia; tale rapporto è pubblicato in formato aperto sul sito istituzionale della Presidenza del Consiglio dei Ministri.
L'Agenzia definisce e aggiorna annualmente le linee guida nazionali che individuano gli standard tecnici, compresa la determinazione delle ontologie dei servizi e dei dati, le procedure e le modalità di attuazione delle disposizioni del Capo V del presente Codice con l'obiettivo di rendere il processo omogeneo a livello nazionale, efficiente ed efficace. Le pubbliche amministrazioni di cui all'articolo 2, comma 2, del presente Codice si uniformano alle suddette linee guida.
Il Presidente del Consiglio o il Ministro delegato per l'innovazione tecnologica riferisce annualmente al Parlamento sullo stato di attuazione delle disposizioni del presente articolo.
L'Agenzia svolge le attività indicate dal presente articolo con le risorse umane, strumentali, e finanziarie previste a legislazione vigente. (138)(240)

Articolo 53.
Caratteristiche dei siti.

1. Le pubbliche amministrazioni centrali realizzano siti istituzionali su reti telematiche che rispettano i princìpi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità dì consultazione, qualità, omogeneità ed interoperabilità. Sono in particolare resi facilmente reperibili e consultabili i dati di cui all' articolo 54. (139)
2. Il DigitPA svolge funzioni consultive e di coordinamento sulla realizzazione e modificazione dei siti delle amministrazioni centrali. (140)
3. Lo Stato promuove intese ed azioni comuni con le regioni e le autonomie locali affinché realizzino siti istituzionali con le caratteristiche di cui al comma 1.

Articolo 54.
Contenuto dei siti delle pubbliche amministrazioni.

1. I siti delle pubbliche amministrazioni contengono i dati di cui al decreto legislativo recante il riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, adottato ai sensi dell'articolo 1, comma 35, della legge 6 novembre 2012, n. 190. (141)

Articolo 55.
Consultazione delle iniziative normative del Governo.

1. La Presidenza del Consiglio dei Ministri può pubblicare su sito telematico le notizie relative ad iniziative normative del Governo, nonché i disegni di legge di particolare rilevanza, assicurando forme di partecipazione del cittadino in conformità con le disposizioni vigenti in materia di tutela delle persone e di altri soggetti rispetto al trattamento di dati personali. La Presidenza del Consiglio dei Ministri può inoltre pubblicare atti legislativi e regolamentari in vigore, nonché i massimari elaborati da organi di giurisdizione.
2. Con decreto del Presidente del Consiglio dei Ministri sono individuate le modalità di partecipazione del cittadino alla consultazione gratuita in via telematica.

Articolo 56.
Dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado. (152)

1. I dati identificativi delle questioni pendenti dinanzi al giudice amministrativo e contabile sono resi accessibili a chi vi abbia interesse mediante pubblicazione sul sistema informativo interno e sul sito istituzionale delle autorità emananti. (153)
2. Le sentenze e le altre decisioni del giudice amministrativo e contabile, rese pubbliche mediante deposito in segreteria, sono contestualmente inserite nel sistema informativo interno e sul sito istituzionale, osservando le cautele previste dalla normativa in materia di tutela dei dati personali. (154)
2-bis. I dati identificativi delle questioni pendenti, le sentenze e le altre decisioni depositate in cancelleria o segreteria dell'autorità giudiziaria di ogni ordine e grado sono, comunque, rese accessibili ai sensi dell'articolo 51 del codice in materia di protezione dei dati personali approvato con decreto legislativo n. 196 del 2003. (155)

Articolo 57. (156)
Moduli e formulari.

Abrogato (157) (237)

Articolo 57-bis. (158)
Indice degli indirizzi delle pubbliche amministrazioni.

1. Al fine di assicurare la pubblicità dei riferimenti telematici delle pubbliche amministrazioni e dei gestori dei pubblici servizi è istituito l'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. (159)
2. La realizzazione e la gestione dell'indice sono affidate a DigitPA, che può utilizzare a tal fine elenchi e repertori già formati dalle amministrazioni pubbliche. (160)
3. Le amministrazioni aggiornano gli indirizzi e i contenuti dell'indice tempestivamente e comunque con cadenza almeno semestrale secondo le indicazioni di DigitPA. 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. (161) (161-b)

Sezione II
Fruibilità dei dati

Articolo 58.
Modalità della fruibilità del dato.

1. Il trasferimento di un dato da un sistema informativo ad un altro non modifica la titolarità del dato.
2. Ai sensi dell' articolo 50, comma 2, nonché al fine di agevolare l'acquisizione d'ufficio ed il controllo sulle dichiarazioni sostitutive riguardanti informazioni e dati relativi a stati, qualità personali e fatti di cui agli articoli 46 e 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 , le Amministrazioni titolari di banche dati accessibili per via telematica predispongono, sulla base delle linee guida redatte da DigitPA, sentito il Garante per la protezione dei dati personali, 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 convenzioni valgono anche quale autorizzazione ai sensi dell'articolo 43, comma 2, del citato decreto del Presidente della Repubblica n. 445 del 2000. (162)
3. DigitPA provvede al monitoraggio dell'attuazione del presente articolo, riferendo annualmente con apposita relazione al Ministro per la pubblica amministrazione e l'innovazione e alla Commissione per la valutazione, la trasparenza e l'integrità delle amministrazione pubbliche di cui all'articolo 13 del decreto legislativo 27 ottobre 2009, n. 150. (163)
3-bis. In caso di mancata predisposizione delle convenzioni di cui al comma 2, il Presidente del Consiglio dei Ministri stabilisce un termine entro il quale le amministrazioni interessate devono provvedere. Decorso inutilmente il termine, il Presidente del Consiglio dei Ministri può nominare un commissario ad acta incaricato di predisporre le predette convenzioni. Al Commissario non spettano compensi, indennità o rimborsi. (164)
3-ter. Resta ferma la speciale disciplina dettata in materia di dati territoriali. (165)

Articolo 59.
Dati territoriali.

1. Per dato territoriale si intende qualunque informazione geograficamente localizzata.
2. È istituito il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, con il compito di definire le regole tecniche per la realizzazione delle basi dei dati territoriali, la documentazione, la fruibilità e lo scambio dei dati stessi tra le pubbliche amministrazioni centrali e locali in coerenza con le disposizioni del presente decreto che disciplinano il sistema pubblico di connettività. (166)
3. Per agevolare la pubblicità dei dati di interesse generale, disponibili presso le pubbliche amministrazioni a livello nazionale, regionale e locale, presso il DigitPA è istituito il Repertorio nazionale dei dati territoriali. (167)
4. Ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400 , con uno o più decreti sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, previa intesa con la Conferenza unificata di cui all'articolo 8 decreto legislativo 28 agosto 1997, n. 281 , sono definite la composizione e le modalità per il funzionamento del Comitato di cui al comma 2. (168)

5. Con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il Ministro dell'ambiente e della tutela del territorio e del mare, per i profili relativi ai dati ambientali, sentito il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 luglio 1998, n. 281 , sono definite le regole tecniche per la definizione del contenuto del repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di successivo aggiornamento dello stesso, per la formazione, la documentazione e lo scambio dei dati territoriali detenuti dalle singole amministrazioni competenti, nonché le regole ed i costi per l'utilizzo dei dati stessi tra le pubbliche amministrazioni centrali e locali e da parte dei privati. (169)
6. La partecipazione al Comitato non comporta oneri né alcun tipo di spese ivi compresi compensi o gettoni di presenza. Gli eventuali rimborsi per spese di viaggio sono a carico delle amministrazioni direttamente interessate che vi provvedono nell'àmbito degli ordinari stanziamenti di bilancio.
7. Agli oneri finanziari di cui al comma 3 si provvede con il fondo di finanziamento per i progetti strategici del settore informatico di cui all'articolo 27, comma 2, della legge 16 gennaio 2003, n. 3 .
7-bis. Nell'ambito dei dati territoriali di interesse nazionale rientra la base dei dati catastali gestita dall'Agenzia del territorio. Per garantire la circolazione e la fruizione dei dati catastali conformemente alle finalità ed alle condizioni stabilite dall' articolo 50, il direttore dell'Agenzia del territorio, di concerto con il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni e previa intesa con la Conferenza unificata, definisce con proprio decreto entro la data del 30 giugno 2006, in coerenza con le disposizioni che disciplinano il sistema pubblico di connettività, le regole tecnico economiche per l'utilizzo dei dati catastali per via telematica da parte dei sistemi informatici di altre amministrazioni. (170)

Articolo 60.
Base di dati di interesse nazionale.

1. Si definisce base di dati di interesse nazionale l'insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è utilizzabile dalle pubbliche amministrazioni, anche per fini statistici, per l'esercizio delle proprie funzioni e nel rispetto delle competenze e delle normative vigenti. (171)
2. Ferme le competenze di ciascuna pubblica amministrazione, le basi di dati di interesse nazionale costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate. La realizzazione di tali sistemi informativi e le modalità di aggiornamento sono attuate secondo le regole tecniche sul sistema pubblico di connettività di cui all' articolo 73 e secondo le vigenti regole del Sistema statistico nazionale di cui al decreto legislativo 6 settembre 1989, n. 322 , e successive modificazioni. (172)
3. Le basi di dati di interesse nazionale sono individuate con decreto del Presidente del Consiglio dei Ministri, su proposta del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con i Ministri di volta in volta interessati, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281 , nelle materie di competenza e sentiti il Garante per la protezione dei dati personali e l'Istituto nazionale di statistica. Con il medesimo decreto sono altresì individuate le strutture responsabili della gestione operativa di ciascuna base di dati e le caratteristiche tecniche del sistema informativo di cui al comma 2. (173)

3-bis. In sede di prima applicazione e fino all'adozione del decreto di cui al comma 3, sono individuate le seguenti basi di dati di interesse nazionale:
a) repertorio nazionale dei dati territoriali;
b) anagrafe nazionale della popolazione residente; (238)
c) banca dati nazionale dei contratti pubblici di cui all' articolo 62-bis ;
d) casellario giudiziale;
e) registro delle imprese;
f) gli archivi automatizzati in materia di immigrazione e di asilo di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 27 luglio 2004, n. 242. (174)
4. Agli oneri finanziari di cui al presente articolo si provvede con il fondo di finanziamento per i progetti strategici del settore informatico di cui all'articolo 27, comma 2, della legge 16 gennaio 2003, n. 3.

Articolo 61.
Delocalizzazione dei registri informatici.

1. Fermo restando il termine di cui all' articolo 40, comma 4, i pubblici registri immobiliari possono essere formati e conservati su supporti informatici in conformità alle disposizioni del presente codice, secondo le regole tecniche stabilite dall' articolo 71, nel rispetto della normativa speciale e dei princìpi stabiliti dal codice civile . In tal caso i predetti registri possono essere conservati anche in luogo diverso dall'Ufficio territoriale competente.

Articolo 62.
Anagrafe nazionale della popolazione residente - ANPR.

1. E' istituita presso il Ministero dell'interno l'Anagrafe nazionale della popolazione residente (ANPR), quale base di dati di interesse nazionale, ai sensi dell'articolo 60, che subentra all'Indice nazionale delle anagrafi (INA), istituito ai sensi del quinto comma dell'articolo 1 della legge 24 dicembre 1954, n. 1228, recante "Ordinamento delle anagrafi della popolazione residente" e all'Anagrafe della popolazione italiana residente all'estero (AIRE),istituita ai sensi della legge 27 ottobre 1988, n. 470, recante "Anagrafe e censimento degli italiani all'estero". Tale base di dati è sottoposta ad un audit di sicurezza con cadenza annuale in conformità alle regole tecniche di cui all'articolo 51. I risultati dell'audit sono inseriti nella relazione annuale del Garante per la protezione dei dati personali.
2. Ferme restando le attribuzioni del sindaco di cui all'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali, approvato con il decreto legislativo 18 agosto 2000, n. 267, l'ANPR subentra altresì alle anagrafi della popolazione residente e dei cittadini italiani residenti all'estero tenute dai comuni. Con il decreto di cui al comma 6 è definito un piano per il graduale subentro dell'ANPR alle citate anagrafi, da completare entro il 31 dicembre 2014. Fino alla completa attuazione di detto piano, l'ANPR acquisisce automaticamente in via telematica i dati contenuti nelle anagrafi tenute dai comuni per i quali non è ancora avvenuto il subentro. L'ANPR è organizzata secondo modalità funzionali e operative che garantiscono la univocità dei dati stessi.
3. L'ANPR assicura al singolo comune la disponibilità dei dati anagrafici della popolazione residente e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite al sindaco ai sensi dell'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali di cui al decreto legislativo 18 agosto 2000, n. 267, nonché la disponibilità dei dati anagrafici e dei servizi per l'interoperabilità con le banche dati tenute dai comuni per lo svolgimento delle funzioni di competenza. L'ANPR consente esclusivamente ai comuni la certificazione dei dati anagrafici nel

rispetto di quanto previsto dall'articolo 33 del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, anche in modalità telematica. I comuni inoltre possono consentire, anche mediante apposite convenzioni, la fruizione dei dati anagrafici da parte dei soggetti aventi diritto. L'ANPR assicura alle pubbliche amministrazioni e agli organismi che erogano pubblici servizi l'accesso ai dati contenuti nell'ANPR.
4. Con il decreto di cui al comma 6 sono disciplinate le modalità di integrazione nell'ANPR dei dati dei cittadini attualmente registrati in anagrafi istituite presso altre amministrazioni nonché dei dati relativi al numero e alla data di emissione e di scadenza della carta di identità della popolazione residente.
5. Ai fini della gestione e della raccolta informatizzata di dati dei cittadini, le pubbliche amministrazioni di cui all'articolo 2, comma 2, del presente Codice si avvalgono esclusivamente dell'ANPR, che viene integrata con gli ulteriori dati a tal fine necessari.
6. Con uno o più decreti del Presidente del Consiglio dei Ministri, su proposta del Ministro dell'interno, del Ministro per la pubblica amministrazione e la semplificazione e del Ministro delegato all'innovazione tecnologica, di concerto con il Ministro dell'economia e delle finanze, d'intesa con l'Agenzia per l'Italia digitale, la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano nonché la Conferenza Stato - città, di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, per gli aspetti d'interesse dei comuni, sentita l'ISTAT e acquisito il parere del Garante per la protezione dei dati personali, sono stabiliti i tempi e le modalità di attuazione delle disposizioni del presente articolo, anche con riferimento:
a) alle garanzie e alle misure di sicurezza da adottare nel trattamento dei dati personali, alle modalità e ai tempi di conservazione dei dati e all'accesso ai dati da parte delle pubbliche amministrazioni per le proprie finalità istituzionali secondo le modalità di cui all'articolo 58;
b) ai criteri per l'interoperabilità dell'ANPR con le altre banche dati di rilevanza nazionale e regionale, secondo le regole tecniche del sistema pubblico di connettività di cui al capo VIII del presente decreto, in modo che le informazioni di anagrafe, una volta rese dai cittadini, si intendano acquisite dalle pubbliche amministrazioni senza necessità di ulteriori adempimenti o duplicazioni da parte degli stessi;
c) all'erogazione di altri servizi resi disponibili dall'ANPR, tra i quali il servizio di invio telematico delle attestazioni e delle dichiarazioni di nascita e dei certificati di cui all'articolo 74 del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, compatibile con il sistema di trasmissione di cui al decreto del Ministro della salute in data 26 febbraio 2010, pubblicato nella Gazzetta Ufficiale n. 65 del 19 marzo 2010.(175)

Articolo 62-bis. (176)
Banca dati nazionale dei contratti pubblici.

1. Per favorire la riduzione degli oneri amministrativi derivanti dagli obblighi informativi ed assicurare l'efficacia, la trasparenza e il controllo in tempo reale dell'azione amministrativa per l'allocazione della spesa pubblica in lavori, servizi e forniture, anche al fine del rispetto della legalità e del corretto agire della pubblica amministrazione e prevenire fenomeni di corruzione, si utilizza la «Banca dati nazionale dei contratti pubblici» (BDNCP) istituita, presso l'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture, della quale fanno parte i dati previsti dall'articolo 7 del decreto legislativo 12 aprile 2006, n. 163 , e disciplinata, ai sensi del medesimo decreto legislativo, dal relativo regolamento attuativo.

Sezione III
Servizi in rete

Articolo 63.
Organizzazione e finalità dei servizi in rete.

1. Le pubbliche amministrazioni centrali individuano le modalità di erogazione dei servizi in rete in base a criteri di valutazione di efficacia, economicità ed utilità e nel rispetto dei princìpi 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.
2. Le pubbliche amministrazioni e i gestori di servizi pubblici progettano e realizzano 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, in conformità alle regole tecniche da emanare ai sensi dell' articolo 71. Per le amministrazioni e i gestori di servizi pubblici regionali e locali le regole tecniche sono adottate previo parere della Commissione permanente per l'innovazione tecnologica nelle regioni e negli enti locali di cui all' articolo 14, comma 3-bis. (177)
3. Le pubbliche amministrazioni collaborano 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.
3-bis. A partire dal 1° gennaio 2014, allo scopo di incentivare e favorire il processo di informatizzazione e di potenziare ed estendere i servizi telematici, i soggetti di cui all'articolo 2, comma 2, utilizzano esclusivamente i canali e i servizi telematici, ivi inclusa la posta elettronica certificata, per l'utilizzo dei propri servizi, anche a mezzo di intermediari abilitati, per la presentazione da parte degli interessati di denunce, istanze e atti e garanzie fideiussorie, per l'esecuzione di versamenti fiscali, contributivi, previdenziali, assistenziali e assicurativi, nonché per la richiesta di attestazioni e certificazioni.
3-ter. A partire dal 1° gennaio 2014 i soggetti indicati al comma 3-bis utilizzano esclusivamente servizi telematici o la posta elettronica certificata anche per gli atti, le comunicazioni o i servizi dagli stessi resi.
3-quater. I soggetti indicati al comma 3-bis, almeno sessanta giorni prima della data della loro entrata in vigore, pubblicano nel sito web istituzionale l'elenco dei provvedimenti adottati ai sensi dei commi 3-bis e 3-ter, nonché termini e modalità di utilizzo dei servizi e dei canali telematici e della posta elettronica certificata.
3-quinquies. Con decreto del Presidente del Consiglio dei ministri, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e successive modificazioni, da emanare entro sei mesi dalla data di entrata in vigore della presente disposizione, sono stabilite le deroghe e le eventuali limitazioni al principio di esclusività indicato dal comma 3-bis, anche al fine di escludere l'insorgenza di nuovi o maggiori oneri per la finanza pubblica. (177-b)

Articolo 64.
Modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni.

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica. (178)
2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità

elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. Con l'istituzione del sistema SPID di cui al comma 2-bis,le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi solo mediante gli strumenti di cui al comma 1, ovvero mediante servizi offerti dal medesimo sistema SPID.(251) L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni. (179)
2-bis. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).
2-ter. Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, secondo modalità definite con il decreto di cui al comma 2-sexies, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori disservizi in rete, ovvero, direttamente, su richiesta degli interessati.
2-quater. Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-sexies.
2-quinquies. Ai fini dell'erogazione dei propri servizi in rete, è altresì riconosciuta alle imprese, secondo le modalità definite con il decreto di cui al comma 2-sexies, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti. L'adesione al sistema SPID per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera l'impresa da un obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70.
2-sexies.Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali, sono definite le caratteristiche del sistema SPID, anche con riferimento:
a) al modello architetturale e organizzativo del sistema;
b) alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;
c) agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese, compresi gli strumenti di cui al comma 1;
*d)*alle modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;
*e)*ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;
*f)*alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete.(252)
3. Abrogato. (180)

Articolo 65.
Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

1. Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici (247) ai sensi dell' articolo 38 , commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 , sono valide:
a) se sottoscritte mediante la firma digitale o la firma elettronica qualificata, il cui certificato è rilasciato da un certificatore accreditato; (180-b)

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; (181)
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. (182)
1-bis. Con decreto del Ministro per la pubblica amministrazione e l'innovazione e del Ministro per la semplificazione normativa, su proposta dei Ministri competenti per materia, possono essere individuati i casi in cui è richiesta la sottoscrizione mediante firma digitale. (183)
1-ter.Il mancato avvio del procedimento da parte del titolare dell'ufficio competente a seguito di istanza o dichiarazione inviate ai sensi e con le modalità di cui al comma 1, lettere a), c) e c-bis), comporta responsabilità dirigenziale e responsabilità disciplinare dello stesso. (246)
2. Le istanze e le dichiarazioni inviate o compilate sul sito secondo le modalità previste dal comma 1 sono equivalenti alle istanze e alle dichiarazioni sottoscritte con firma autografa apposta in presenza del dipendente addetto al procedimento. (184)
3. Abrogato. (185)
4. Il comma 2 dell'articolo 38 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 , è sostituito dal seguente:
«2. Le istanze e le dichiarazioni inviate per via telematica sono valide se effettuate secondo quanto previsto dall' articolo 65 del decreto legislativo 7 marzo 2005, n. 82».

Sezione IV
Carte elettroniche

Articolo 66.
Carta d'identità elettronica e carta nazionale dei servizi.

1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica e dell'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento dell'età prevista dalla legge per il rilascio della carta d'identità elettronica, sono definite con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, con il Ministro per l'innovazione e le tecnologie e con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281. (186)
2. Le caratteristiche e le modalità per il rilascio, per la diffusione e l'uso della carta nazionale dei servizi sono definite con uno o più regolamenti, ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, adottati su proposta congiunta dei Ministri per la funzione pubblica e per

l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281 , nel rispetto dei seguenti princìpi:
a) all'emissione della carta nazionale dei servizi provvedono, su richiesta del soggetto interessato, le pubbliche amministrazioni che intendono rilasciarla;
b) l'onere economico di produzione e rilascio della carta nazionale dei servizi è a carico delle singole amministrazioni che le emettono;
c) eventuali indicazioni di carattere individuale connesse all'erogazione dei servizi al cittadino, sono possibili nei limiti di cui al decreto legislativo 30 giugno 2003, n. 196;
d) le pubbliche amministrazioni che erogano servizi in rete devono consentirne l'accesso ai titolari della carta nazionale dei servizi indipendentemente dall'ente di emissione, che è responsabile del suo rilascio;
e) la carta nazionale dei servizi può essere utilizzata anche per i pagamenti informatici tra soggetti privati e pubbliche amministrazioni, secondo quanto previsto dalla normativa vigente.
3. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento dell'età prevista dalla legge per il rilascio della carta d'identità elettronica, devono contenere: (187)
a) i dati identificativi della persona;
b) il codice fiscale.
4. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento dell'età prevista dalla legge per il rilascio della carta d'identità elettronica, possono contenere, a richiesta dell'interessato ove si tratti di dati sensibili: (188)
a) l'indicazione del gruppo sanguigno;
b) le opzioni di carattere sanitario previste dalla legge;
c) i dati biometrici indicati col decreto di cui al comma 1, con esclusione, in ogni caso, del DNA;
d) tutti gli altri dati utili al fine di razionalizzare e semplificare l'azione amministrativa e i servizi resi al cittadino, anche per mezzo dei portali, nel rispetto della normativa in materia di riservatezza;
e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica.
5. La carta d'identità elettronica e la carta nazionale dei servizi possono essere utilizzate quali strumenti di autenticazione telematica per l'effettuazione di pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalità stabilite con le regole tecniche di cui all' articolo 71, di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.
6. Con decreto del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281 , sono dettate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta di identità elettronica, del documento di identità elettronico e della carta nazionale dei servizi, nonché le modalità di impiego.
7. Nel rispetto della disciplina generale fissata dai decreti di cui al presente articolo e delle vigenti disposizioni in materia di protezione dei dati personali, le pubbliche amministrazioni, nell'àmbito dei rispettivi ordinamenti, possono sperimentare modalità di utilizzazione dei documenti di cui al presente articolo per l'erogazione di ulteriori servizi o utilità.
8. Le tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del decreto del Presidente della Repubblica 28 luglio 1967, n. 851 , possono essere realizzate anche con modalità elettroniche e contenere le funzionalità della carta nazionale dei servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni.

8-bis. Fino al 31 dicembre 2011, la carta nazionale dei servizi e le altre carte elettroniche ad essa conformi possono essere rilasciate anche ai titolari di carta di identità elettronica. (189)

Capo VI
Sviluppo, acquisizione e riuso di sistemi informatici nelle pubbliche amministrazioni

Articolo 67.
Modalità di sviluppo ed acquisizione.

1. Le pubbliche amministrazioni centrali, per i progetti finalizzati ad appalti di lavori e servizi ad alto contenuto di innovazione tecnologica, possono selezionare uno o più proposte utilizzando il concorso di idee di cui all'articolo 57 del decreto del Presidente della Repubblica 21 dicembre 1999, n. 554 .
2. Le amministrazioni appaltanti possono porre a base delle gare aventi ad oggetto la progettazione, o l'esecuzione, o entrambe, degli appalti di cui al comma 1, le proposte ideative acquisite ai sensi del comma 1, previo parere tecnico di congruità del DigitPA; alla relativa procedura è ammesso a partecipare, ai sensi dell'articolo 57, comma 6, del decreto del Presidente della Repubblica 21 dicembre 1999, n. 554 , anche il soggetto selezionato ai sensi del comma 1, qualora sia in possesso dei relativi requisiti soggettivi. (190)

Articolo 68.
Analisi comparativa delle soluzioni.

1. Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:
a) software sviluppato per conto della pubblica amministrazione;
b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;
c) software libero o a codice sorgente aperto;
d) software fruibile in modalità cloud computing;
e) software di tipo proprietario mediante ricorso a licenza d'uso;
f) software combinazione delle precedenti soluzioni.
1-bis.A tal fine, le pubbliche amministrazioni prima di procedere all'acquisto, secondo le procedure di cui al codice di cui al decreto legislativo 12 aprile 2006 n. 163, effettuano una valutazione comparativa delle diverse soluzioni disponibili sulla base dei seguenti criteri:
a) costo complessivo del programma o soluzione quale costo di acquisto, di implementazione, di mantenimento e supporto;
b) livello di utilizzo di formati di dati e di interfacce di tipo aperto nonché di standard in grado di assicurare l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione;
c) garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio tenuto conto della tipologia di software acquisito.
1-ter Ove dalla valutazione comparativa di tipo tecnico ed economico, secondo i criteri di cui al comma 1-bis, risulti motivatamente l'impossibilità di accedere a soluzioni già disponibili all'interno della pubblica amministrazione, o a software liberi o a codici sorgente aperto, adeguati alle esigenze da soddisfare, è consentita l'acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso. La valutazione di cui al presente comma è effettuata secondo le

modalità e i criteri definiti dall'Agenzia per l'Italia digitale, che, a richiesta di soggetti interessati, esprime altresì parere circa il loro rispetto. (191)
2. Le pubbliche amministrazioni nella predisposizione o nell'acquisizione dei programmi informatici, adottano soluzioni informatiche, quando possibile modulari, basate sui sistemi funzionali resi noti ai sensi dell' articolo 70, che assicurino l'interoperabilità e la cooperazione applicativa e consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto, salvo che ricorrano motivate ed eccezionali esigenze. (192)
2-bis. Le amministrazioni pubbliche comunicano tempestivamente al DigitPA l'adozione delle applicazioni informatiche e delle pratiche tecnologiche, e organizzative, adottate, fornendo ogni utile informazione ai fini della piena conoscibilità delle soluzioni adottate e dei risultati ottenuti, anche per favorire il riuso e la più ampia diffusione delle migliori pratiche. (193)
3. Agli effetti del presente decreto legislativo si intende per:
a) formato dei dati di tipo aperto, un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi;
b) dati di tipo aperto, i dati che presentano le seguenti caratteristiche:
1) sono disponibili secondo i termini di una licenza che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato;
2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera a), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati;
3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione. L'Agenzia per l'Italia digitale deve stabilire, con propria deliberazione, i casi eccezionali, individuati secondo criteri oggettivi, trasparenti e verificabili, in cui essi sono resi disponibili a tariffe superiori ai costi marginali. In ogni caso, l'Agenzia, nel trattamento dei casi eccezionali individuati, si attiene alle indicazioni fornite dalla direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, sul riutilizzo dell'informazione del settore pubblico, recepita con il decreto legislativo 24 gennaio 2006, n. 36 (241)
4. Il DigitPA istruisce ed aggiorna, con periodicità almeno annuale, un repertorio dei formati aperti utilizzabili nelle pubbliche amministrazioni e delle modalità di trasferimento dei formati. (194)

Articolo 69.
Riuso dei programmi informatici.

1. Le pubbliche amministrazioni che siano titolari di programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno obbligo di darli in formato sorgente, completi della documentazione disponibile, in uso gratuito ad altre pubbliche amministrazioni che li richiedono e che intendano adattarli alle proprie esigenze, salvo motivate ragioni. (195)
2. Al fine di favorire il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni, ai sensi del comma 1, nei capitolati o nelle specifiche di progetto è previsto ove possibile, che i programmi appositamente sviluppati per conto e a spese dell'amministrazione siano facilmente portabili su altre piattaforme e conformi alla definizione e regolamentazione effettuata da DigitPA, ai sensi dell' articolo 68, comma 2. (196)
3. Le pubbliche amministrazioni inseriscono, nei contratti per l'acquisizione di programmi informatici o di singoli moduli, di cui al comma 1, clausole che garantiscano il diritto di disporre dei programmi ai fini del riuso da parte della medesima o di altre amministrazioni. (197)

4. Nei contratti di acquisizione di programmi informatici sviluppati per conto e a spese delle amministrazioni, le stesse possono includere clausole, concordate con il fornitore, che tengano conto delle caratteristiche economiche ed organizzative di quest'ultimo, volte a vincolarlo, per un determinato lasso di tempo, a fornire, su richiesta di altre amministrazioni, servizi che consentono il riuso dei programmi o dei singoli moduli. Le clausole suddette definiscono le condizioni da osservare per la prestazione dei servizi indicati. (198)

Articolo 70.
Banca dati dei programmi informatici riutilizzabili.

1. DigitPA, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, valuta e rende note applicazioni tecnologiche realizzate dalle pubbliche amministrazioni, idonee al riuso da parte di altre pubbliche amministrazioni anche con riferimento a singoli moduli, segnalando quelle che, in base alla propria valutazione, si configurano quali migliori pratiche organizzative e tecnologiche. (199)
2. Le pubbliche amministrazioni centrali che intendono acquisire programmi applicativi valutano preventivamente la possibilità di riuso delle applicazioni analoghe rese note dal DigitPA ai sensi del comma 1 , motivandone l'eventuale mancata adozione. (200)

Capo VII
Regole tecniche

Articolo 71.
Regole tecniche.

1. Le regole tecniche previste nel presente codice sono dettate, con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con i Ministri competenti, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281 , ed il Garante per la protezione dei dati personali nelle materie di competenza, previa acquisizione obbligatoria del parere tecnico di DigitPA. (201)
1-bis. Abrogato. (202)
1-ter. Le regole tecniche di cui al presente codice sono dettate in conformità ai requisiti tecnici di accessibilità di cui all'articolo 11 della legge 9 gennaio 2004, n. 4, (244) alle discipline risultanti dal processo di standardizzazione tecnologica a livello internazionale ed alle normative dell'Unione europea. (203)
2. Le regole tecniche vigenti nelle materie del presente codice restano in vigore fino all'adozione delle regole tecniche adottate ai sensi del presente articolo.

Capo VIII
Sistema pubblico di connettività e rete internazionale della pubblica amministrazione (204)

Sezione I
Definizioni relative al sistema pubblico di connettività

Articolo 72.
Definizioni relative al sistema pubblico di connettività.

1. Ai fini del presente decreto si intende per:

a) «trasporto di dati»: i servizi per la realizzazione, gestione ed evoluzione di reti informatiche per la trasmissione di dati, oggetti multimediali e fonia;
b) «interoperabilità di base»: i servizi per la realizzazione, gestione ed evoluzione di strumenti per lo scambio di documenti informatici fra le pubbliche amministrazioni e tra queste e i cittadini;
c) «connettività»: l'insieme dei servizi di trasporto di dati e di interoperabilità di base;
d) «interoperabilità evoluta»: i servizi idonei a favorire la circolazione, lo scambio di dati e informazioni, e l'erogazione fra le pubbliche amministrazioni e tra queste e i cittadini;
e) «cooperazione applicativa»: la parte del sistema pubblico di connettività finalizzata all'interazione tra i sistemi informatici delle pubbliche amministrazioni per garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi.

Articolo 73.
Sistema pubblico di connettività (SPC).

1. Nel rispetto dell'articolo 117, secondo comma, lettera r), della Costituzione , e nel rispetto dell'autonomia dell'organizzazione interna delle funzioni informative delle regioni e delle autonomie locali il presente Capo definisce e disciplina il Sistema pubblico di connettività (SPC), al fine di assicurare il coordinamento informativo e informatico dei dati tra le amministrazioni centrali, regionali e locali e promuovere l'omogeneità nella elaborazione e trasmissione dei dati stessi, finalizzata allo scambio e diffusione delle informazioni tra le pubbliche amministrazioni e alla realizzazione di servizi integrati.
2. Il SPC è l'insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, necessarie per assicurare l'interoperabilità di base ed evoluta e la cooperazione applicativa dei sistemi informatici e dei flussi informativi, garantendo la sicurezza, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.
3. La realizzazione del SPC avviene nel rispetto dei seguenti principi:
a) sviluppo architetturale ed organizzativo atto a garantire la natura federata, policentrica e non gerarchica del sistema;
b) economicità nell'utilizzo dei servizi di rete, di interoperabilità e di supporto alla cooperazione applicativa;
c) sviluppo del mercato e della concorrenza nel settore delle tecnologie dell'informazione e della comunicazione.
3-bis. Le regole tecniche del Sistema pubblico di connettività sono dettate ai sensi dell'articolo 71. (205)

Articolo 74.
Rete internazionale delle pubbliche amministrazioni.

1. Il presente decreto definisce e disciplina la Rete internazionale delle pubbliche amministrazioni, interconnessa al SPC. La Rete costituisce l'infrastruttura di connettività che collega, nel rispetto della normativa vigente, le pubbliche amministrazioni con gli uffici italiani all'estero, garantendo adeguati livelli di sicurezza e qualità.

Sezione II
Sistema pubblico di connettività SPC

Articolo 75.
Partecipazione al Sistema pubblico di connettività.

1. Al SPC partecipano tutte le amministrazioni di cui all' articolo 2, comma 2 .
2. Il comma 1 non si applica alle amministrazioni di cui al decreto legislativo 30 marzo 2001, n. 165, limitatamente all'esercizio delle sole funzioni di ordine e sicurezza pubblica, difesa nazionale, consultazioni elettorali.
3. Ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 11 novembre 1994, n. 680 , nonché dell'articolo 25 del decreto legislativo 30 giugno 2003, n. 196 , è comunque garantita la connessione con il SPC dei sistemi informativi degli organismi competenti per l'esercizio delle funzioni di sicurezza e difesa nazionale, nel loro esclusivo interesse e secondo regole tecniche che assicurino riservatezza e sicurezza. È altresì garantita la possibilità di connessione al SPC delle autorità amministrative indipendenti.
3-bis. Il gestore di servizi pubblici e i soggetti che perseguono finalità di pubblico interesse possono usufruire della connessione al SPC e dei relativi servizi, adeguandosi alle vigenti regole tecniche, previa delibera della Commissione di cui all' articolo 79. (206)

Articolo 76.
Scambio di documenti informatici nell'ambito del Sistema pubblico di connettività.

1. 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.

Articolo 77.
Finalità del Sistema pubblico di connettività.

1. Al SPC sono attribuite le seguenti finalità:
a) fornire un insieme di servizi di connettività condivisi dalle pubbliche amministrazioni interconnesse, definiti negli aspetti di funzionalità, qualità e sicurezza, ampiamente graduabili in modo da poter soddisfare le differenti esigenze delle pubbliche amministrazioni aderenti al SPC;
b) garantire l'interazione della pubblica amministrazione centrale e locale con tutti gli altri soggetti connessi a Internet, nonché con le reti di altri enti, promuovendo l'erogazione di servizi di qualità e la miglior fruibilità degli stessi da parte dei cittadini e delle imprese;
c) fornire un'infrastruttura condivisa di interscambio che consenta l'interoperabilità tra tutte le reti delle pubbliche amministrazioni esistenti, favorendone lo sviluppo omogeneo su tutto il territorio nella salvaguardia degli investimenti effettuati;
d) fornire servizi di connettività e cooperazione alle pubbliche amministrazioni che ne facciano richiesta, per permettere l'interconnessione delle proprie sedi e realizzare così anche l'infrastruttura interna di comunicazione;
e) realizzare un modello di fornitura dei servizi multifornitore coerente con l'attuale situazione di mercato e le dimensioni del progetto stesso;
f) garantire lo sviluppo dei sistemi informatici nell'ambito del SPC salvaguardando la sicurezza dei dati, la riservatezza delle informazioni, nel rispetto dell'autonomia del patrimonio informativo delle singole amministrazioni e delle vigenti disposizioni in materia di protezione dei dati personali.

Articolo 78.

Compiti delle pubbliche amministrazioni nel Sistema pubblico di connettività.

1. Le pubbliche amministrazioni nell'ambito della loro autonomia funzionale e gestionale adottano nella progettazione e gestione dei propri sistemi informativi, ivi inclusi gli aspetti organizzativi, soluzioni tecniche compatibili con la cooperazione applicativa con le altre pubbliche amministrazioni, secondo le regole tecniche di cui all' articolo 73, comma 3-bis. Le stesse pubbliche amministrazioni, ove venga loro attribuito, per norma, il compito di gestire soluzioni infrastrutturali per l'erogazione di servizi comuni a più amministrazioni, adottano le medesime regole per garantire la compatibilità con la cooperazione applicativa potendosi avvalere di modalità atte a mantenere distinti gli ambiti di competenza. (207)
2. Per le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39 , le responsabilità di cui al comma 1 sono attribuite al dirigente responsabile dei sistemi informativi automatizzati, di cui all'articolo 10, comma 1, dello stesso decreto legislativo.
2-bis. Le pubbliche amministrazioni centrali e periferiche di cui all' articolo 1, comma 1, lettera z), del presente codice, inclusi gli istituti e le scuole di ogni ordine e grado, le istituzioni educative e le istituzioni universitarie, nei limiti di cui all'articolo 1, comma 449, secondo periodo, della legge 27 dicembre 2006, n. 296 , sono tenute, a decorrere dal 1° gennaio 2008 e comunque a partire dalla scadenza dei contratti relativi ai servizi di fonia in corso alla data predetta ad utilizzare i servizi «Voce tramite protocollo Internet» (VoIP) previsti dal sistema pubblico di connettività o da analoghe convenzioni stipulate da CONSIP. (208)
2-ter. Il DigitPA effettua azioni di monitoraggio e verifica del rispetto delle disposizioni di cui al comma 2-bis. (209)
2-quater. Il mancato adeguamento alle disposizioni di cui al comma 2-bis comporta la riduzione, nell'esercizio finanziario successivo, del 30 per cento delle risorse stanziate nell'anno in corso per spese di telefonia. (210)

Articolo 79.
Commissione di coordinamento del Sistema pubblico di connettività.

1. È istituita la Commissione di coordinamento del SPC, di seguito denominata: «Commissione», preposta agli indirizzi strategici del SPC.
2. La Commissione:
a) assicura il raccordo tra le amministrazioni pubbliche, nel rispetto delle funzioni e dei compiti spettanti a ciascuna di esse;
b) approva le linee guida, le modalità operative e di funzionamento dei servizi e delle procedure per realizzare la cooperazione applicativa fra i servizi erogati dalle amministrazioni;
c) promuove l'evoluzione del modello organizzativo e dell'architettura tecnologica del SPC in funzione del mutamento delle esigenze delle pubbliche amministrazioni e delle opportunità derivanti dalla evoluzione delle tecnologie;
d) promuove la cooperazione applicativa fra le pubbliche amministrazioni, nel rispetto delle regole tecniche di cui all' articolo 71;
e) definisce i criteri e ne verifica l'applicazione in merito alla iscrizione, sospensione e cancellazione dagli elenchi dei fornitori qualificati SPC di cui all'articolo 82;
f) dispone la sospensione e cancellazione dagli elenchi dei fornitori qualificati di cui all'articolo 82;
g) verifica la qualità e la sicurezza dei servizi erogati dai fornitori qualificati del SPC;
h) promuove il recepimento degli standard necessari a garantire la connettività, l'interoperabilità di base e avanzata, la cooperazione applicativa e la sicurezza del Sistema.

3. Le decisioni della Commissione sono assunte a maggioranza semplice o qualificata dei componenti in relazione all'argomento in esame. La Commissione a tale fine elabora, entro tre mesi dal suo insediamento, un regolamento interno da approvare con maggioranza qualificata dei suoi componenti.

Articolo 80.
Composizione della Commissione di coordinamento del sistema pubblico di connettività.

1. La Commissione è formata da diciassette componenti incluso il Presidente di cui al comma 2, scelti tra persone di comprovata professionalità ed esperienza nel settore, nominati con decreto del Presidente del Consiglio dei Ministri: otto componenti sono nominati in rappresentanza delle amministrazioni statali previa deliberazione del Consiglio dei Ministri, sette dei quali su proposta del Ministro per l'innovazione e le tecnologie ed uno su proposta del Ministro per la funzione pubblica; i restanti otto sono nominati su designazione della Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281 . Uno dei sette componenti proposti dal Ministro per l'innovazione e le tecnologie è nominato in rappresentanza della Presidenza del Consiglio dei Ministri. Quando esamina questioni di interesse della rete internazionale della pubblica amministrazione la Commissione è integrata da un rappresentante del Ministero degli affari esteri, qualora non ne faccia già parte.
2. Il Presidente della Commissione è il Commissario del Governo per l'attuazione dell'agenda digitale o, su sua delega, il Direttore dell'Agenzia digitale. Il Presidente e gli altri componenti della Commissione restano in carica per un triennio e l'incarico è rinnovabile. (211)
3. La Commissione è convocata dal Presidente e si riunisce almeno quattro volte l'anno.
4. L'incarico di Presidente o di componente della Commissione e la partecipazione alle riunioni della Commissione non danno luogo alla corresponsione di alcuna indennità, emolumento, compenso e rimborso spese e le amministrazioni interessate provvedono agli oneri di missione nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica.
5. Per i necessari compiti istruttori la Commissione si avvale del DigitPA, di seguito denominato "DigitPA", e sulla base di specifiche convenzioni, di organismi interregionali e territoriali. (212)
6. La Commissione può avvalersi, nell'ambito delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente, senza nuovi o maggiori oneri per la finanza pubblica, della consulenza di uno o più organismi di consultazione e cooperazione istituiti con appositi accordi ai sensi dell'articolo 9, comma 2, lettera c), del decreto legislativo 28 agosto 1997, n. 281 .
7. Ai fini della definizione degli sviluppi strategici del SPC, in relazione all'evoluzione delle tecnologie dell'informatica e della comunicazione, la Commissione può avvalersi, nell'ambito delle risorse finanziarie assegnate al DigitPA a legislazione vigente e senza nuovi o maggiori oneri per la finanza pubblica, di consulenti di chiara fama ed esperienza in numero non superiore a cinque secondo le modalità definite nei regolamenti di cui all' articolo 87. (213)

Articolo 81.
Ruolo del DigitPA (214)

1. Il DigitPA, nel rispetto delle decisioni e degli indirizzi forniti dalla Commissione, anche avvalendosi di soggetti terzi, gestisce le risorse condivise del SPC e le strutture operative preposte al controllo e supervisione delle stesse, per tutte le pubbliche amministrazioni di cui all' articolo 2, comma 2. (215)

2. Il DigitPA, anche avvalendosi di soggetti terzi, cura la progettazione, la realizzazione, la gestione e l'evoluzione del SPC per le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39. (216)
2-bis. Al fine di dare attuazione a quanto disposto dall'articolo 5, DigitPA, mette a disposizione, attraverso il Sistema pubblico di connettività, una piattaforma tecnologica per l'interconnessione e l'interoperabilità tra le pubbliche amministrazioni e i prestatori di servizi di pagamento abilitati, al fine di assicurare, attraverso strumenti condivisi di riconoscimento unificati, l'autenticazione certa dei soggetti interessati all'operazione in tutta la gestione del processo di pagamento. (217)

Articolo 82.
Fornitori del Sistema pubblico di connettività.

1. Sono istituiti uno o più elenchi di fornitori a livello nazionale e regionale in attuazione delle finalità di cui all' articolo 77.
2. I fornitori che ottengono la qualificazione SPC ai sensi dei regolamenti previsti dall' articolo 87, sono inseriti negli elenchi di competenza nazionale o regionale, consultabili in via telematica, esclusivamente ai fini dell'applicazione della disciplina di cui al presente decreto, e tenuti rispettivamente dal DigitPA a livello nazionale e dalla regione di competenza a livello regionale. I fornitori in possesso dei suddetti requisiti sono denominati fornitori qualificati SPC. (218)
3. I servizi per i quali è istituito un elenco, ai sensi del comma 1, sono erogati, nell'ambito del SPC, esclusivamente dai soggetti che abbiano ottenuto l'iscrizione nell'elenco di competenza nazionale o regionale.
4. Per l'iscrizione negli elenchi dei fornitori qualificati SPC è necessario che il fornitore soddisfi almeno i seguenti requisiti:
a) disponibilità di adeguate infrastrutture e servizi di comunicazioni elettroniche;
b) esperienza comprovata nell'ambito della realizzazione gestione ed evoluzione delle soluzioni di sicurezza informatica;
c) possesso di adeguata rete commerciale e di assistenza tecnica;
d) possesso di adeguati requisiti finanziari e patrimoniali, anche dimostrabili per il tramite di garanzie rilasciate da terzi qualificati.
5. Limitatamente ai fornitori dei servizi di connettività dovranno inoltre essere soddisfatti anche i seguenti requisiti:
a) possesso dei necessari titoli abilitativi di cui al decreto legislativo 1° agosto 2003, n. 259 , per l'ambito territoriale di esercizio dell'attività;
b) possesso di comprovate conoscenze ed esperienze tecniche nella gestione delle reti e servizi di comunicazioni elettroniche, anche sotto il profilo della sicurezza e della protezione dei dati.

Articolo 83.
Contratti quadro.

1. Al fine della realizzazione del SPC, il DigitPA a livello nazionale e le regioni nell'ambito del proprio territorio, per soddisfare esigenze di coordinamento, qualificata competenza e indipendenza di giudizio, nonché per garantire la fruizione, da parte delle pubbliche amministrazioni, di elevati livelli di disponibilità dei servizi e delle stesse condizioni contrattuali proposte dal miglior offerente, nonché una maggiore affidabilità complessiva del sistema, promuovendo, altresì, lo sviluppo della concorrenza e assicurando la presenza di più fornitori qualificati, stipulano, espletando specifiche procedure ad evidenza pubblica per la selezione dei contraenti, nel rispetto delle vigenti norme in materia, uno o più contratti-quadro con più fornitori

per i servizi di cui all' articolo 77, con cui i fornitori si impegnano a contrarre con le singole amministrazioni alle condizioni ivi stabilite. (219)
2. Le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39 , sono tenute a stipulare gli atti esecutivi dei contratti-quadro con uno o più fornitori di cui al comma 1, individuati dal DigitPA. Gli atti esecutivi non sono soggetti al parere del DigitPA e, ove previsto, del Consiglio di Stato. Le amministrazioni non ricomprese tra quelle di cui al citato art. 1, comma 1, del decreto legislativo n. 39 del 1993 , hanno facoltà di stipulare gli atti esecutivi di cui al presente articolo. (220)

Articolo 84.
Migrazione della Rete unitaria della pubblica amministrazione.

1. Le Amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39 , aderenti alla Rete unitaria della pubblica amministrazione, presentano al DigitPA, secondo le indicazioni da esso fornite, i piani di migrazione verso il SPC, da attuarsi entro diciotto mesi dalla data di approvazione del primo contratto quadro di cui all'articolo 83, comma 1, termine di cessazione dell'operatività della Rete unitaria della pubblica amministrazione. (221)
2. Dalla data di entrata in vigore del presente articolo ogni riferimento normativo alla Rete unitaria della pubblica amministrazione si intende effettuato al SPC.

Sezione III
Rete internazionale della pubblica amministrazione e compiti di DigitPA (222)

Articolo 85.
Collegamenti operanti per il tramite della Rete internazionale delle pubbliche amministrazioni.

1. Le amministrazioni di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39 , che abbiano l'esigenza di connettività verso l'estero, sono tenute ad avvalersi dei servizi offerti dalla Rete internazionale delle pubbliche amministrazioni, interconnessa al SPC.
2. Le pubbliche amministrazioni di cui al comma 1, che dispongono di reti in ambito internazionale sono tenute a migrare nella Rete internazionale delle pubbliche amministrazioni entro il 15 marzo 2007, fatto salvo quanto previsto dall' articolo 75 , commi 2 e 3.
3. Le amministrazioni non ricomprese tra quelle di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39 , ivi incluse le autorità amministrative indipendenti, possono aderire alla Rete internazionale delle pubbliche amministrazioni.

Articolo 86.
Compiti e oneri del DigitPA. (223)

1. Il DigitPA cura la progettazione, la realizzazione, la gestione ed evoluzione della Rete internazionale delle pubbliche amministrazioni, previo espletamento di procedure concorsuali ad evidenza pubblica per la selezione dei fornitori e mediante la stipula di appositi contratti-quadro secondo modalità analoghe a quelle di cui all' articolo 83. (224)
2. Il DigitPA, al fine di favorire una rapida realizzazione del SPC, per un periodo almeno pari a due anni a decorrere dalla data di approvazione dei contratti-quadro di cui all' articolo 83, comma 1, sostiene i costi delle infrastrutture condivise, a valere sulle risorse già previste nel bilancio dello Stato. (225)

3. Al termine del periodo di cui al comma 2, i costi relativi alle infrastrutture condivise sono a carico dei fornitori proporzionalmente agli importi dei contratti di fornitura, e una quota di tali costi è a carico delle pubbliche amministrazioni relativamente ai servizi da esse utilizzati. I costi, i criteri e la relativa ripartizione tra le amministrazioni sono determinati annualmente con decreto del Presidente del Consiglio dei Ministri, su proposta della Commissione, previa intesa con la Conferenza unificata cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, salvaguardando eventuali intese locali finalizzate a favorire il pieno ingresso nel SPC dei piccoli Comuni nel rispetto di quanto previsto dal comma 5 .
4. Il DigitPA sostiene tutti gli oneri derivanti dai collegamenti in ambito internazionale delle amministrazioni di cui all' articolo 85, comma 1, per i primi due anni di vigenza contrattuale, decorrenti dalla data di approvazione del contratto quadro di cui all' articolo 83; per gli anni successivi ogni onere è a carico della singola amministrazione contraente proporzionalmente ai servizi acquisiti. (226)
5. Le amministrazioni non ricomprese tra quelle di cui all'articolo 1, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, che aderiscono alla Rete internazionale delle pubbliche amministrazioni, ai sensi dell' articolo 85, comma 3, ne sostengono gli oneri relativi ai servizi che utilizzano.

Articolo 87.
Regolamenti.

1. Ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400 , con uno o più decreti sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281 , sono adottati regolamenti per l'organizzazione del SPC, per l'avvalimento dei consulenti di cui all' articolo 80, comma 7, e per la determinazione dei livelli minimi dei requisiti richiesti per l'iscrizione agli elenchi dei fornitori qualificati del SPC di cui all' articolo 82.

Capo IX (227)
Disposizioni transitorie finali e abrogazioni

Articolo 88. (228)
Norme transitorie per la firma digitale.

1. I documenti sottoscritti con firma digitale basata su certificati rilasciati da certificatori iscritti nell'elenco pubblico già tenuto dall'Autorità per l'informatica nella pubblica amministrazione sono equivalenti ai documenti sottoscritti con firma digitale basata su certificati rilasciati da certificatori accreditati .

Articolo 89. (229)
Aggiornamenti.

1. La Presidenza del Consiglio dei Ministri adotta gli opportuni atti di indirizzo e di coordinamento per assicurare che i successivi interventi normativi, incidenti sulle materie oggetto di riordino siano attuati esclusivamente mediante la modifica o l'integrazione delle disposizioni contenute nel presente codice .

Articolo 90. (230)
Oneri finanziari.

1. All'attuazione del presente decreto si provvede nell'àmbito delle risorse previste a legislazione vigente.

Articolo 91. (231)
Abrogazioni.

1. Dalla data di entrata in vigore del presente testo unico sono abrogati:
a) il decreto legislativo 23 gennaio 2002, n. 10 ;
b) gli articoli 1, comma 1, lettere t), u), v), z), aa), bb), cc), dd), ee), ff), gg), hh), ii), ll), mm), nn), oo); 2, comma 1, ultimo periodo; 6; 8; 9; 10; 11; 12; 13; 14; 17; 20; 22; 23; 24; 25; 26; 27; 27-bis; 28; 28-bis; 29; 29-bis; 29-ter; 29-quater; 29-quinquies; 29-sexies; 29-septies; 29-octies; 36, commi 1, 2, 3, 4, 5 e 6; 51; del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A);
c) l'articolo 26, comma 2 , lettere a), e), h), della legge 27 dicembre 2002, n. 289 ;
d) articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3 ;
e) gli articoli 16, 17, 18 e 19 della legge 29 luglio 2003, n. 229 .
2. Le abrogazioni degli articoli 2, comma 1, ultimo periodo, 6, commi 1 e 2; 10; 36, commi 1, 2, 3, 4, 5 e 6 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A), si intendono riferite anche al decreto legislativo 28 dicembre 2000, n. 443 (Testo B).
3. Le abrogazioni degli articoli 1, comma 1, lettere t), u), v), z), aa), bb), cc), dd), ee), ff), gg), hh), ii), ll), mm), nn), oo); 6, commi 3 e 4; 8; 9; 11; 12; 13; 14; 17; 20; 22; 23; 24; 25; 26; 27; 27-bis; 28; 28-bis; 29; 29-bis; 29-ter; 29-quater; 29-quinquies; 29-sexies; 29-septies; 29-octies; 51 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo A), si intendono riferite anche al decreto del Presidente della Repubblica 28 dicembre 2000, n. 444 (Testo C).
3-bis. L'articolo 15, comma 1, della legge 15 marzo 1997, n. 59 , è abrogato. (232)
3-ter. Il decreto legislativo 28 febbraio 2005, n. 42 , è abrogato. (233)

Articolo 92.
Entrata in vigore del codice.

1. Le disposizioni del presente codice entrano in vigore a decorrere dal 1° gennaio 2006.

Note della redazione:

(1) - Lettera prima modificata dall'art. 1, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituita dalla lettera a) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(2) - Lettera così modificata dalla lettera b) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(3) - Lettera così modificata dall'art. 1, D.Lgs. 4 aprile 2006, n. 159.

(4) - Lettera integrata da lettera c) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(5) - Lettera integrata dalla lettera c) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(6) - Lettera integrata dalla lettera c) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(7) - Lettera integrata dalla lettera c) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(8) - Lettera integrata dalla lettera d) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(9) - Lettera così modificata dall'art. 1, D.Lgs. 4 aprile 2006, n. 159.

(10) - Lettera integrata dalla lettera e) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(11) - Lettera prima modificata dall'art. 1, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituita dalla lettera f) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(12) - Lettera così sostituita dalla lettera g) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(13) - Lettera integrata dalla lettera h) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(14) - Lettera integrata dalla lettera h) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(15) - Lettera aggiunta dalla lettera i) del comma 1 dell'art. 1, D.Lgs. 30 dicembre 2010, n. 235.

(16) - Si veda anche l'art. 48, D.L. 25 giugno 2008, n. 112.

(17) - Comma così sostituito dalla lettera a) del comma 1 dell'art. 2, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, il comma 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(18) - Comma abrogato dalla lettera b) del comma 1 dell'art. 2, D.Lgs. 30 dicembre 2010, n. 235.

(19) - Comma così sostituito dalla lettera c) del comma 1 dell'art. 2, D.Lgs. 30 dicembre 2010, n. 235.

(20) - Comma così modificato dall'art. 2, D.Lgs. 4 aprile 2006, n. 159.

(21) - Comma così modificato dalla lettera d) del comma 1 dell'art. 2, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, il comma 1 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010. In attuazione di quanto disposto dal presente comma vedi, per l'Agenzia delle entrate, il D.P.C.M. 2 marzo 2011; per la Presidenza del Consiglio dei Ministri, il D.P.C.M. 9 febbraio 2011.

(22) - Comma così modificato prima dall'art. 3, D.Lgs. 4 aprile 2006, n. 159 e poi dalla lettera a) del comma 1 dell'art. 3, D.Lgs. 30 dicembre 2010, n. 235.

(23) - Comma abrogato dalla lettera b) del comma 1 dell'art. 3, D.Lgs. 30 dicembre 2010, n. 235.

(24) - Comma integrato dall'art. 3, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituito dal comma 17 dell'art. 3 dell'allegato 4 al D.Lgs. 2 luglio 2010, n. 104, a decorrere dal 16 settembre 2010, ai sensi di quanto disposto dall'art. 2 dello stesso provvedimento.

(25) - Articolo integralmente sostituito dal comma 1 dell'art. 15, D.L. 18 ottobre 2012, n. 179.

(26) - Articolo integrato dal comma 2 dell'art. 4, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, il comma 3 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(27) - Comma così sostituito dalla lettera a) del comma 1 dell'art. 5, D.Lgs. 30 dicembre 2010, n. 235.

(28) - Comma integrato dalla lettera b) del comma 1 dell'art. 5, D.Lgs. 30 dicembre 2010, n. 235. Si veda, anche, il comma 4 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(29) - Comma abrogato dalla lettera c) del comma 1 dell'art. 5, D.Lgs. 30 dicembre 2010, n. 235.

(30) - Comma abrogato dalla lettera c) del comma 1 dell'art. 5, D.Lgs. 30 dicembre 2010, n. 235.

(31) - Comma così modificato dal comma 1 dell'art. 6, D.Lgs. 30 dicembre 2010, n. 235.

(32) - Comma così modificato dal comma 1 dell'art. 7, D.Lgs. 30 dicembre 2010, n. 235.

(33) - Rubrica così sostituita dalla lettera a) del comma 1 dell'art. 8, D.Lgs. 30 dicembre 2010, n. 235.

(34) - Comma così sostituito dalla lettera b) del comma 1 dell'art. 8, D.Lgs. 30 dicembre 2010, n. 235.

(35) - Comma abrogato dalla lettera c) del comma 1 dell'art. 8, D.Lgs. 30 dicembre 2010, n. 235.

(36) - Comma abrogato dalla lettera c) del comma 1 dell'art. 8, D.Lgs. 30 dicembre 2010, n. 235.

(37) - Comma così modificato dall'art. 4, D.Lgs. 4 aprile 2006, n. 159.

(38) - Per l'attuazione di quanto disposto dal comma si veda il D.P.C.M. 3 aprile 2006, n. 200.

(39) - Comma così modificato dalla lettera a) del comma 1 dell'art. 9, D.Lgs. 30 dicembre 2010, n. 235.

(40) - Comma aggiunto dall'art. 5, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituito dalla lettera b) del comma 1 dell'art. 9, D.Lgs. 30 dicembre 2010, n. 235.

(41) - Comma aggiunto dall'art. 5, D.Lgs. 4 aprile 2006, n. 159 e poi così modificato dalla lettera c) del comma 1 dell'art. 9, D.Lgs. 30 dicembre 2010, n. 235.

(42) - Comma così modificato dalla lettera d) del comma 1 dell'art. 9, D.Lgs. 30 dicembre 2010, n. 235. si veda, anche, il comma 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(43) - Comma aggiunto dall'art. 5, D.Lgs. 4 aprile 2006, n. 159 e poi così modificato dalla lettera e) del comma 1 dell'art. 9, D.Lgs. 30 dicembre 2010, n. 235. si veda, anche, il comma 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(44) - Comma integrato dal comma 1 dell'art. 10, D.Lgs. 30 dicembre 2010, n. 235.

(45) - Comma integrato dal comma 1 dell'art. 10, D.Lgs. 30 dicembre 2010, n. 235.

(46) - Comma aggiunto dall'art. 6, D.Lgs. 4 aprile 2006, n. 159.

(47) - Comma integrato dal comma 1 dell'art. 11, D.Lgs. 30 dicembre 2010, n. 235

(48) - Comma integrato dal comma 1 dell'art. 11, D.Lgs. 30 dicembre 2010, n. 235.

(49) - In tema di specifiche tecniche per la trasmissione dei dati ai fini della cooperazione applicativa con i servizi di emergenza si veda il D.M. 17 giugno 2008 (pubblicato in G.U. 3 luglio 2008, n. 154)

(49-b) - Articolo così integrato dall'art.47 -ter del decreto-legge 9 febbraio 2012 n.5 come modificato in sede di conversione.

(50) - Alinea così sostituito dalla lettera a) del comma 1 dell'art. 12, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, i commi 5 e 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(51) - Lettera così modificata dal numero 1) della lettera b) del comma 1 dell'art. 12, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, i commi 5 e 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(52) - Lettera così modificata dal numero 2) della lettera b) del comma 1 dell'art. 12, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, i commi 5 e 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(53) - Lettera così sostituita dal numero 3) della lettera b) del comma 1 dell'art. 12, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, i commi 5 e 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(54) - Lettera così modificata dal numero 4) della lettera b) del comma 1 dell'art. 12, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, i commi 5 e 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(55) - Lettera così modificata dal numero 5) della lettera b) del comma 1 dell'art. 12, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, i commi 5 e 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(56) - Comma integrato dall'art. 7, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituito dalla lettera c) del comma 1 dell'art. 12, D.Lgs. 30 dicembre 2010, n. 235. Si veda, anche, il comma 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(57) - Comma integrato dalla lettera d) del comma 1 dell'art. 12, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, il comma 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(58) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(59) - Rubrica così modificata e sostituita dal comma 1 dell'art. 17 e dal comma 1 dell'art. 26, D.Lgs. 30 dicembre 2010, n. 235.

(60) - Comma così modificato prima dall'art. 8, D.Lgs. 4 aprile 2006, n. 159 e poi dalla lettera a) del comma 1 dell'art. 13, D.Lgs. 30 dicembre 2010, n. 235.

(61) - Comma integrato dall'art. 8, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituito dalla lettera b) del comma 1 dell'art. 13, D.Lgs. 30 dicembre 2010, n. 235.

(62) - Comma abrogato dalla lettera c) del comma 1 dell'art. 13, D.Lgs. 30 dicembre 2010, n. 235.

(63) - Comma prima modificato dall'art. 8, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituito dalla lettera d) del comma 1 dell'art. 13, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, il comma 6 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(64) - Comma integrato dalla lettera e) del comma 1 dell'art. 13, D.Lgs. 30 dicembre 2010, n. 235.

(65) - Rubrica così sostituita dalla lettera a) del comma 1 dell'art. 14, D.Lgs. 30 dicembre 2010, n. 235.

(66) - Comma così modificato dall'art. 9, D.Lgs. 4 aprile 2006, n. 159.

(67) - Comma prima modificato dall'art. 9, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituito, con gli attuali commi 2 e 2-bis, dalla lettera b) del comma 1 dell'art. 14, D.Lgs. 30 dicembre 2010, n. 235.

(68) - Comma integrato dalla lettera b) del comma 1 dell'art. 14, D.Lgs. 30 dicembre 2010, n. 235.

(69) - Articolo prima modificato dall'art. 10, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituito dal comma 1 dell'art. 15, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, il comma 7 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(70) - Articolo prima modificato dall'art. 11, D.Lgs. 4 aprile 2006, n. 159 e dal comma 12 dell'art. 16, D.L. 29 novembre 2008, n. 185 e poi così sostituito dal comma 1 dell'art. 16, D.Lgs. 30 dicembre 2010, n. 235.

(71) - Articolo integrato dal comma 2 dell'art. 16, D.Lgs. 30 dicembre 2010, n. 235.

(72) - Articolo integrato dal comma 2 dell'art. 16, D.Lgs. 30 dicembre 2010, n. 235. si veda, anche, il comma 8 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(73) - Articolo integrato dal comma 2 dell'art. 16, D.Lgs. 30 dicembre 2010, n. 235.

(74) - Articolo così sostituito dal comma 2 dell'art. 17, D.Lgs. 30 dicembre 2010, n. 235.

(75) - Comma così modificato dal comma 1 dell'art. 18, D.Lgs. 30 dicembre 2010, n. 235.

(76) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(77) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(78) - Lettera così modificata dall'art. 12, D.Lgs. 4 aprile 2006, n. 159.

(79) - Alinea così modificato dall'art. 12, D.Lgs. 4 aprile 2006, n. 159.

(80) - Lettera così modificata dall'art. 12, D.Lgs. 4 aprile 2006, n. 159.

(81) - Lettera così sostituita dall'art. 12, D.Lgs. 4 aprile 2006, n. 159.

(82) - Comma integrato dal comma 1 dell'art. 19, D.Lgs. 30 dicembre 2010, n. 235. Si veda, anche, il comma 9 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(83) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(84) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(85) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(86) - Comma così sostituito dal comma 1 dell'art. 20, D.Lgs. 30 dicembre 2010, n. 235.

(87) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(88) - Comma così modificato dall'art. 13, D.Lgs. 4 aprile 2006, n. 159.

(89) - Articolo così sostituito dal comma 1 dell'art. 21, D.Lgs. 30 dicembre 2010, n. 235.

(90) - Comma così modificato dall'art. 14, D.Lgs. 4 aprile 2006, n. 159.

(91) - Comma così modificato dall'art. 14, D.Lgs. 4 aprile 2006, n. 159.

(92) - Lettera soppressa dalla lettera a) del comma 1 dell'art. 22, D.Lgs. 30 dicembre 2010, n. 235.

(93) - Lettera così modificata dall'art. 14, D.Lgs. 4 aprile 2006, n. 159.

(94) - Lettera integrata dalla lettera b) del comma 1 dell'art. 22, D.Lgs. 30 dicembre 2010, n. 235.

(95) - Articolo integrato dal comma 2 dell'art. 22, D.Lgs. 30 dicembre 2010, n. 235.

(96) - Comma così modificato dal comma 1 dell'art. 23, D.Lgs. 30 dicembre 2010, n. 235.

(97) - Lettera così modificata dall'art. 15, D.Lgs. 4 aprile 2006, n. 159.

(98) - Comma così modificato dall'art. 15, D.Lgs. 4 aprile 2006, n. 159.

(99) - Comma così sostituito dalla lettera a) del comma 1 dell'art. 24, D.Lgs. 30 dicembre 2010, n. 235.

(100) - Comma così sostituito dalla lettera a) del comma 1 dell'art. 24, D.Lgs. 30 dicembre 2010, n. 235.

(101) - Comma così modificato dai numeri 1) e 2) della lettera b) del comma 1 dell'art. 24, D.Lgs. 30 dicembre 2010, n. 235.

(102) - Comma così sostituito dalla lettera c) del comma 1 dell'art. 24, D.Lgs. 30 dicembre 2010, n. 235.

(103) - Lettera così modificata dall'art. 16, D.Lgs. 4 aprile 2006, n. 159.

(104) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(105) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(106) - Comma integrato dal comma 1 dell'art. 25, D.Lgs. 30 dicembre 2010, n. 235.

(107) - Rubrica così sostituita prima dall'art. 17, D.Lgs. 4 aprile 2006, n. 159 e poi dal comma 1 dell'art. 26, D.Lgs. 30 dicembre 2010, n. 235.

(108) - Rubrica così sostituita dal comma 2 dell'art. 26, D.Lgs. 30 dicembre 2010, n. 235.

(109) - Comma così modificato dalla lettera a) del comma 1 dell'art. 27, D.Lgs. 30 dicembre 2010, n. 235.

(110) - Comma abrogato dalla lettera b) del comma 1 dell'art. 27, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, il comma 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(111) - Articolo integrato dal comma 2 dell'art. 27, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, il comma 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(112) - Comma integrato dalla lettera a) del comma 1 dell'art. 28, D.Lgs. 30 dicembre 2010, n. 235.

(113) - Comma così modificato dalla lettera b) del comma 1 dell'art. 28, D.Lgs. 30 dicembre 2010, n. 235. Si veda, anche, il comma 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(114) - Comma integrato dall'art. 18, D.Lgs. 4 aprile 2006, n. 159 e poi così modificato dalla lettera c) del comma 1 dell'art. 28, D.Lgs. 30 dicembre 2010, n. 235.

(115) - Comma aggiunto dall'art. 18, D.Lgs. 4 aprile 2006, n. 159.

(116) - Lettera integrata dalla lettera d) del comma 1 dell'art. 28, D.Lgs. 30 dicembre 2010, n. 235.

(117) - Comma integrato dall'art. 18, D.Lgs. 4 aprile 2006, n. 159.

(118) - Comma così modificato dalla lettera a) del comma 1 dell'art. 29, D.Lgs. 30 dicembre 2010, n. 235.

(119) - Comma così modificato dalla lettera b) del comma 1 dell'art. 29, D.Lgs. 30 dicembre 2010, n. 235.

(120) - Alinea così modificato dalla lettera a) del comma 1 dell'art. 30, D.Lgs. 30 dicembre 2010, n. 235.

(121) - Comma integrato dalla lettera b) del comma 1 dell'art. 30, D.Lgs. 30 dicembre 2010, n. 235.

(122) - Comma integrato dalla lettera b) del comma 1 dell'art. 30, D.Lgs. 30 dicembre 2010, n. 235.

(123) - Articolo integrato dal comma 2 dell'art. 30, D.Lgs. 30 dicembre 2010, n. 235.

(124) - Comma così modificato dal comma 1 dell'art. 31, D.Lgs. 30 dicembre 2010, n. 235.

(125) - Comma così modificato dalla lettera a) del comma 1 dell'art. 32, D.Lgs. 30 dicembre 2010, n. 235.

(126) - Lettera così modificata dalla lettera b) del comma 1 dell'art. 32, D.Lgs. 30 dicembre 2010, n. 235.

(127) - Comma prima modificato dall'art. 19, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituito dalla lettera c) del comma 1 dell'art. 32, D.Lgs. 30 dicembre 2010, n. 235.

(128) - Articolo così sostituito dal comma 1 dell'art. 33, D.Lgs. 30 dicembre 2010, n. 235.

(129) - In merito ad applicabilità delle disposizioni contenute nel presente comma limitatamente all'Agenzia delle Entrate, si veda comma 2 dell'art. 3, D.P.C.M. 2 marzo 2011.

(130) - Comma così modificato dal comma 1 dell'art. 34, D.Lgs. 30 dicembre 2010, n. 235.

(131) - Comma così modificato dall'art. 20, D.Lgs. 4 aprile 2006, n. 159.

(132) - Articolo integrato dal comma 2 dell'art. 34, D.Lgs. 30 dicembre 2010, n. 235. Vedi, anche, i commi 10 e 20 dell'art. 57 dello stesso D.Lgs. n. 235 del 2010.

(133) - Rubrica così sostituita dalla lettera a) del comma 1 dell'art. 35, D.Lgs. 30 dicembre 2010, n. 235.

(134) - Comma così sostituito dalla lettera b) del comma 1 dell'art. 35, D.Lgs. 30 dicembre 2010, n. 235.

(135) - Comma integrato dalla lettera c) del comma 1 dell'art. 35, D.Lgs. 30 dicembre 2010, n. 235.

(136) - Comma integrato dalla lettera d) del comma 1 dell'art. 35, D.Lgs. 30 dicembre 2010, n. 235.

(137) - Rubrica così modificata dalla lettera a) del comma 1 dell'art. 36, D.Lgs. 30 dicembre 2010, n. 235.

(138) - Articolo così sostituito dalla lettera a) del comma 1 dell'art. 9, D.L. 18 ottobre 2012, n.179.

(139) - Periodo aggiunto dall'art. 21, D.Lgs. 4 aprile 2006, n. 159.

(140) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(141) - Articolo così sostituito dall'art. 52, comma 3, D.Lgs. 14 marzo 2013, n. 33.

(142) - Lettera così modificata dall'art. 22, D.Lgs. 4 aprile 2006, n. 159.

(143) - Lettera così modificata dalla lettera a) del comma 1 dell'art. 37, D.Lgs. 30 dicembre 2010, n. 235.

(144) - Lettera integrata dalla lettera b) del comma 1 dell'art. 37, D.Lgs. 30 dicembre 2010, n. 235.

(145) - Comma integrato dalla lettera c) del comma 1 dell'art. 37, D.Lgs. 30 dicembre 2010, n. 235.

(146) - Comma abrogato dalla lettera d) del comma 1 dell'art. 37, D.Lgs. 30 dicembre 2010, n. 235.

(147) - Comma abrogato dalla lettera d) del comma 1 dell'art. 37, D.Lgs. 30 dicembre 2010, n. 235.

(148) - Comma integrato dalla lettera b) del comma 1 dell'art. 34, L. 18 giugno 2009, n. 69 e poi così sostituito dalla lettera e) del comma 1 dell'art. 37, D.Lgs. 30 dicembre 2010, n. 235.

(149) - Comma integrato dalla lettera b) del comma 1 dell'art. 34, L. 18 giugno 2009, n. 69 e poi così modificato dalla lettera f) del comma 1 dell'art. 37, D.Lgs. 30 dicembre 2010, n. 235.

(150) - Comma così modificato dalla lettera g) del comma 1 dell'art. 37, D.Lgs. 30 dicembre 2010, n. 235

(151) - Comma integrato dall'art. 22, D.Lgs. 4 aprile 2006, n. 159.

(152) - Rubrica così modificata dall'art. 23, D.Lgs. 4 aprile 2006, n. 159.

(153) - Comma così modificato dalla lettera a) del comma 1 dell'art. 38, D.Lgs. 30 dicembre 2010, n. 235.

(154) - Comma così modificato dalla lettera b) del comma 1 dell'art. 38, D.Lgs. 30 dicembre 2010, n. 235.

(155) - Comma integrato dall'art. 23, D.Lgs. 4 aprile 2006, n. 159.

(156) - Riferimento in nota non più valido. Vedi nota successiva.

(157) - Articolo abrogato dall’ art. 53, comma 1, lett. f), D.Lgs. 14 marzo 2013, n. 33.

(158) - Articolo integrato dall'art. 17, comma 29, D.L. 1° luglio 2009, n. 78, come modificato dalla relativa legge di conversione.

(159) - Comma così sostituito dalla lettera d-bis) del comma 1 dell'art. 6, D.L. 18 ottobre 2012, n. 179, nel testo integrato dalla legge di conversione 17 dicembre 2012, n. 221.

(160) - Comma così sostituito dalla lettera b) del comma 1 dell'art. 40, D.Lgs. 30 dicembre 2010, n. 235.

(161) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(161-b) - Comma così sostituito dall'art.47-ter del decreto-legge 9 febbraio 2012 n.5 come modificato in sede di conversione.

(162) - Comma così sostituito dalla lettera a) del comma 1 dell'art. 41, D.Lgs. 30 dicembre 2010, n. 235.

(163) - Comma prima modificato dall'art. 24, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituito dalla lettera b) del comma 1 dell'art. 41, D.Lgs. 30 dicembre 2010, n. 235.

(164) - Comma integrato dalla lettera c) del comma 1 dell'art. 41, D.Lgs. 30 dicembre 2010, n. 235.

(165) - Comma aggiunto dalla lettera c) del comma 1 dell'art. 41, D.Lgs. 30 dicembre 2010, n. 235.

(166) - Comma così modificato dall'art. 25, D.Lgs. 4 aprile 2006, n. 159.

(167) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(168) - In attuazione di quanto disposto dal presente comma, si veda il D.M. 2 maggio 2006, n. 237.

(169) - Comma così modificato prima dall'art. 5, comma 4, D.Lgs. 27 gennaio 2010, n. 32 e poi dal comma 1 dell'art. 42, D.Lgs. 30 dicembre 2010, n. 235.

(170) - Comma integrato dall'art. 25, D.Lgs. 4 aprile 2006, n. 159.

(171) - Comma così modificato dalla lettera a) del comma 1 dell'art. 43, D.Lgs. 30 dicembre 2010, n. 235.

(172) - Comma così modificato dalla lettera b) del comma 1 dell'art. 43, D.Lgs. 30 dicembre 2010, n. 235.

(173) - Comma così modificato dalla lettera c) del comma 1 dell'art. 43, D.Lgs. 30 dicembre 2010, n. 235.

(174) - Comma integrato dalla lettera d) del comma 1 dell'art. 43, D.Lgs. 30 dicembre 2010, n. 235.

(175) - Articolo così modificato dal comma 1 dell'art. 2, D.L. 18 ottobre 2012, n. 179.

(176) - Articolo integrato dal comma 1 dell'art. 44, D.Lgs. 30 dicembre 2010, n. 235.

(177) - Comma così sostituito dal comma 1 dell'art. 45, D.Lgs. 30 dicembre 2010, n. 235.

(177-b) - Articolo così integrato dall'art.47 -quinquies del decreto-legge 9 febbraio 2012 n.5 come modificato in sede di conversione.

(178) - Comma così modificato dalla lettera a) del comma 1 dell'art. 46, D.Lgs. 30 dicembre 2010, n. 235.

(179) - Comma così modificato dalla lettera b) del comma 1 dell'art. 46, D.Lgs. 30 dicembre 2010, n. 235.

(180) - Comma abrogato dalla lettera c) del comma 1 dell'art. 46, D.Lgs. 30 dicembre 2010, n. 235.

(180-b) - Lettera così modificata dall'art.47 -sexies del decreto-legge 9 febbraio 2012 n.5 come modificato in sede di conversione.

(181) - Lettera così modificata dalla lettera a) del comma 1 dell'art. 47, D.Lgs. 30 dicembre 2010, n. 235.

(182) - Lettera integrata dall'art. 17, comma 28, D.L. 1° luglio 2009, n. 78 e poi così sostituita dalla lettera b) del comma 1 dell'art. 47, D.Lgs. 30 dicembre 2010, n. 235.

(183) - Comma integrato dalla lettera c) del comma 1 dell'art. 47, D.Lgs. 30 dicembre 2010, n. 235.

(184) - Comma così modificato prima dall'art. 28, D.Lgs. 4 aprile 2006, n. 159 e poi dalla lettera d) del comma 1 dell'art. 47, D.Lgs. 30 dicembre 2010, n. 235.

(185) - Comma abrogato dalla lettera e) del comma 1 dell'art. 47, D.Lgs. 30 dicembre 2010, n. 235.

(186) - Comma così modificato dal comma 1 dell'art. 48, D.Lgs. 30 dicembre 2010, n. 235.

(187) - Alinea così modificato dal comma 1 dell'art. 48, D.Lgs. 30 dicembre 2010, n. 235.

(188) - Alinea così modificato dal comma 1 dell'art. 48, D.Lgs. 30 dicembre 2010, n. 235.

(189) - Comma integrato dal comma 1 dell'art. 37, L. 18 giugno 2009, n. 69 e poi così modificato dal comma 101 dell'art. 2, L. 23 dicembre 2009, n. 191, a decorrere dal 1° gennaio 2010 ai sensi di quanto disposto dal comma 253 del citato art. 2 della medesima L. 23 dicembre 2009, n. 191

(190) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(191) - Comma così sostituito dall'articolo 9-bis comma 1 D.L. 18 ottobre 2012, n.179 convertito in legge con modificazioni dalla l. 17 dicembre 2012, n. 221

(192) - Comma così sostituito dalla lettera b) del comma 1 dell'art. 49, D.Lgs. 30 dicembre 2010, n. 235.

(193) - Comma integrato dalla lettera c) del comma 1 dell'art. 49, D.Lgs. 30 dicembre 2010, n. 235.

(194) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(195) - Comma così modificato dalla lettera a) del comma 1 dell'art. 50, D.Lgs. 30 dicembre 2010, n. 235.

(196) - Comma così modificato dalla lettera b) del comma 1 dell'art. 50, D.Lgs. 30 dicembre 2010, n. 235.

(197) - Comma così modificato dalla lettera c) del comma 1 dell'art. 50, D.Lgs. 30 dicembre 2010, n. 235.

(198) - Comma così modificato dalla lettera d) del comma 1 dell'art. 50, D.Lgs. 30 dicembre 2010, n. 235.

(199) - Comma così sostituito dalla lettera a) del comma 1 dell'art. 51, D.Lgs. 30 dicembre 2010, n. 235.

(200) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(201) - Comma prima modificato dall'art. 29, D.Lgs. 4 aprile 2006, n. 159 e poi così sostituito dalla lettera a) del comma 1 dell'art. 52, D.Lgs. 30 dicembre 2010, n. 235.

(202) - Comma abrogato dalla lettera b) del comma 1 dell'art. 52, D.Lgs. 30 dicembre 2010, n. 235.

(203) - Comma integrato dall'art. 29, D.Lgs. 4 aprile 2006, n. 159.

(204) - L'attuale Capo VIII, che include gli articoli da 72 a 87, è stato integrato dall'art. 30, D.Lgs. 4 aprile 2006, n. 159.

(205) - Comma integrato dal comma 1 dell'art. 53, D.Lgs. 30 dicembre 2010, n. 235.

(206) - Comma aggiunto dal comma 1 dell'art. 54, D.Lgs. 30 dicembre 2010, n. 235.

(207) - Comma così modificato dalle lettere a) e b) del comma 1 dell'art. 55, D.Lgs. 30 dicembre 2010, n. 235.

(208) - Comma integrato dal comma 591 dell'art. 2, L. 24 dicembre 2007, n. 244.

(209) - Comma integrato dal comma 591 dell'art. 2, L. 24 dicembre 2007, n. 244 e poi così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(210) - Comma integrato dal comma 591 dell'art. 2, L. 24 dicembre 2007, n. 244.

(211) - Comma così modificato ai sensi di quanto disposto dal comma 1 dell'art. 15, D.L. 21 giugno 2013, n. 69.

(212) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(213) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(214) - Rubrica così modificata ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(215) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(216) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(217) - Comma integrato dal comma 5 dell'art. 6, D.L. 13 agosto 2011, n. 138.

(218) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(219) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(220) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(221) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(222) - Rubrica così modificata ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(223) - Rubrica così modificata ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235

(224) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235

(225) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(226) - Comma così modificato ai sensi di quanto disposto dal comma 18 dell'art. 57, D.Lgs. 30 dicembre 2010, n. 235.

(227) - Capo così rinumerato dall'art. 31, D.Lgs. 4 aprile 2006, n. 159.

(228) - Articolo così rinumerato dall'art. 31, D.Lgs. 4 aprile 2006, n. 159.

(229) - Articolo così rinumerato dall'art. 31, D.Lgs. 4 aprile 2006, n. 159.

(230) - Articolo così rinumerato dall'art. 31, D.Lgs. 4 aprile 2006, n. 159.

(231) - Articolo così rinumerato dall'art. 31, D.Lgs. 4 aprile 2006, n. 159.

(232) - Comma integrato dall'art. 32, D.Lgs. 4 aprile 2006, n. 159.

(233) - Comma integrato dall'art. 32, D.Lgs. 4 aprile 2006, n. 159.

(234) - Comma così modificato dalla lettera b) del comma 6 dell'art. 9, D.L. 18 ottobre 2012, n. 179.

(235) - Comma così integrato dalla lettera c) del comma 6 dell'art. 9, D.L. 18 ottobre 2012, n. 179.

(236) - lettera integrata dal comma 2 dell'art. 9, D.L. 18 ottobre 2012, n. 179.

(237) - riferimento in nota non più valido. Vedi nota 157

(238) - lettera così modificata dal comma 2 dell'art. 2, D.L. 18 ottobre 2012, n. 179.

(239) - integrazione così effettuata dalla lettera d) del comma 1 dell'art. 6, D.L. 18 ottobre 2012, n. 179.

(240) - ai sensi dell’art. 9 comma 3 D.L. 18 ottobre 2012, n. 179 in sede di prima applicazione, i regolamenti di cui all'articolo 52, comma 1, sono pubblicati entro 120 giorni dalla data di entrata in vigore della legge di conversione del presente decreto-legge. Con riferimento ai documenti e ai dati già pubblicati, la disposizione di cui all'articolo 52, comma 2, trova applicazione entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto.

(241) - Comma così sostituito dalla lettera b) del comma 1 dell’art. 9, D.L. 18 ottobre 2012, n. 179, come modificata dalla legge di conversione 17 dicembre 2012, n. 221 .

(242) - integrazione effettuata dalla lettera a) del comma 6 dell'art. 9, D.L. 18 ottobre 2012, n. 179.

(243) - integrazione effettuata dalla lettera a) del comma 1 dell'art. 6, D.L. 18 ottobre 2012, n. 179.

(244) - integrazione effettuata dalla lettera f) del comma 6 dell'art. 9, D.L. 18 ottobre 2012, n. 179.

(245) - integrazione effettuata dalla lettera d) del comma 6 dell'art. 9, D.L. 18 ottobre 2012, n. 179.

(246) - integrazione effettuata dalla lettera b) del comma 1 dell'art. 6, D.L. 18 ottobre 2012, n. 179.

(247) - integrazione effettuata dalla lettera c) del comma 1 dell'art. 6, D.L. 18 ottobre 2012, n. 179.

(248) - articolo introdotto dal comma 1 dell'art. 4, D.L. 18 ottobre 2012, n. 179.

(249) - articolo introdotto dal comma 3 dell'art. 5, D.L. 18 ottobre 2012, n. 179.

(250) - Comma così modificato dall'art.14 comma 1-ter del D.L. 21 giugno 2013 n 69 convertito con modificazioni dalla L. 9 agosto 2013, n. 98.

(251) - Comma così modificato dall'art.17-ter comma 1 del D.L. 21 giugno 2013 n 69 convertito con modificazioni dalla L. 9 agosto 2013, n. 98.

(252) - Comma così modificato dall'art.17-ter comma 2 del D.L. 21 giugno 2013 n 69 convertito con modificazioni dalla L. 9 agosto 2013, n. 98.

16.2 - Decreto Ministeriale 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.

Capo I
PRINCIPI GENERALI

IL MINISTRO DELLA GIUSTIZIA di concerto con IL MINISTRO PER LA PUBBLICA AMMINISTRAZIONE E L'INNOVAZIONE

Visto l'articolo 17, comma 3, della legge 23 agosto 1988, n. 400;
Visto l'articolo 4 del decreto-legge 29 dicembre 2009, n. 193, recante «Interventi urgenti in materia di funzionalità del sistema giudiziario», convertito in legge, con modificazioni, dalla legge 22 febbraio 2010 n.24;
Visto il decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni;
Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali» e successive modificazioni;
Visti gli articoli 16 e 16-bis del decreto-legge 29 novembre 2008 n. 185 recante «Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale», convertito in legge, con modificazioni, dalla legge 28 gennaio 2009, n. 2 »;
Visto il decreto del Presidente della Repubblica 13 febbraio 2001, n. 123, recante «Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti»;
Visto il decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, recante «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge n. 16 gennaio 2003, n. 3»;
Visto il decreto del Ministro della giustizia 17 luglio 2008, recante «Regole tecnico operative per l'uso di strumenti informatici e telematici nel processo civile»;
Visto il decreto ministeriale 27 aprile 2009 recante «Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia»; Visto il decreto del presidente del

consiglio dei ministri 6 maggio 2009, recante «Disposizioni in materia di rilascio e di uso della casella di posta elettronica
certificata assegnata ai cittadini»;
Rilevata la necessità di adottare le regole tecniche previste dall'articolo 4, comma 1, del citato decreto, in sostituzione delle regole tecniche adottate con il decreto del Presidente della Repubblica 13 febbraio 2001, n. 123 e con il decreto del Ministro della Giustizia 17 luglio 2008;
Acquisito il parere espresso in data 15 luglio 2010 dal Garante per la protezione dei dati personali;
Acquisito il parere espresso in data 20 luglio 2010 da DigitPA;
Udito il parere del Consiglio di Stato, espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 25 novembre 2010 e quello espresso nell'adunanza del 20 dicembre 2010;
Vista la comunicazione al Presidente del Consiglio dei Ministri in data 18 gennaio 2011;

A d o t t a

il seguente regolamento:

Art. 1
Ambito di applicazione

1. Il presente decreto stabilisce le regole tecniche per l'adozione nel processo civile e nel processo penale delle tecnologie dell'informazione e della comunicazione ai sensi dell'articolo 4, comma 1, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24, recante «Interventi urgenti in materia di funzionalità del sistema giudiziario» ed in attuazione del decreto legislativo 7 marzo 2005, n. 82,
recante «Codice dell'amministrazione digitale» e successive modificazioni.

Art. 2
Definizioni

1. Ai fini del presente decreto si intendono per:
a) dominio giustizia: l'insieme delle risorse hardware e software, mediante il quale il Ministero della giustizia tratta in via informatica e telematica qualsiasi tipo di attività, di dato, di servizio, di comunicazione e di procedura;
b) portale dei servizi telematici: struttura tecnologica-organizzativa che fornisce l'accesso ai servizi telematici resi disponibili dal dominio giustizia, secondo le regole tecnico-operative riportate nel presente decreto;
c) punto di accesso: struttura tecnologica-organizzativa che fornisce ai soggetti abilitati esterni al dominio giustizia i servizi di connessione al portale dei servizi telematici, secondo le regole tecnico-operative riportate nel presente decreto;
d) gestore dei servizi telematici: sistema informatico, interno al dominio giustizia, che consente l'interoperabilità tra i sistemi informatici utilizzati dai soggetti abilitati interni, il portale dei servizi telematici e il gestore di posta elettronica certificata del Ministero della giustizia;
e) posta elettronica certificata: sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici, di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68;
f) identificazione informatica: operazione di identificazione in rete del titolare della carta nazionale dei servizi o di altro dispositivo crittografico, mediante un certificato di autenticazione, secondo la definizione di cui al decreto legislativo 7 marzo 2005, n. 82;

g) firma digitale: firma elettronica avanzata, basata su un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura, di cui al decreto legislativo 7 marzo 2005, n. 82;
h) fascicolo informatico: versione informatica del fascicolo d'ufficio, contenente gli atti del processo come documenti informatici, oppure le copie informatiche dei medesimi atti, qualora siano stati depositati su supporto cartaceo, ai sensi del codice dell'amministrazione digitale;
i) codice dell'amministrazione digitale (CAD): decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni;
l) codice in materia di protezione dei dati personali: decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" e successive modificazioni;
m) soggetti abilitati: i soggetti abilitati all'utilizzo dei servizi di consultazione di informazioni e trasmissione di documenti informatici relativi al processo. In particolare si intende per:
1) soggetti abilitati interni: i magistrati, il personale degli uffici giudiziari e degli UNEP;
2) soggetti abilitati esterni: i soggetti abilitati esterni privati e i soggetti abilitati esterni pubblici;
3) soggetti abilitati esterni privati: i difensori delle parti private, gli avvocati iscritti negli elenchi speciali, gli esperti e gli ausiliari del giudice;
4) soggetti abilitati esterni pubblici: gli avvocati, i procuratori dello Stato e gli altri dipendenti di amministrazioni statali, regionali, metropolitane, provinciali e comunali;
n) utente privato: la persona fisica o giuridica, quando opera al di fuori dei casi previsti dalla lettera m);
o) certificazione del soggetto abilitato esterno privato: attestazione di iscrizione all'albo, all'albo speciale, al registro ovvero di possesso della qualifica che legittima l'esercizio delle funzioni professionali e l'assenza di cause ostative all'accesso;
p) certificazione del soggetto abilitato esterno pubblico: attestazione di appartenenza del soggetto all'amministrazione pubblica e dello svolgimento di funzioni tali da legittimare l'accesso;
q) specifiche tecniche: le disposizioni di carattere tecnico emanate, ai sensi dell'articolo 34, dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia, sentito DigitPA e il Garante per la protezione dei dati personali, limitatamente ai profili inerenti la protezione dei dati personali;
r) spam: messaggi indesiderati;
s) software antispam: software studiato e progettato per rilevare ed eliminare lo spam;
t) log: documento informatico contenente la registrazione cronologica di una o più operazioni informatiche, generato automaticamente dal sistema informatico;
u) richiesta di pagamento telematico (RPT): struttura standardizzata che definisce gli elementi necessari a caratterizzare il pagamento e qualifica il versamento con un identificativo univoco, nonché contiene i dati identificativi, variabili secondo il tipo di operazione, e una parte riservata per inserire informazioni elaborabili automaticamente dai sistemi informatici;
v) ricevuta telematica (RT): struttura standardizzata, emessa a fronte di una RPT, che definisce gli elementi necessari a qualificare il pagamento e trasferisce inalterate le informazioni della RPT relative alla parte riservata;
z) identificativo univoco di erogazione del servizio (CRS): identifica univocamente una richiesta di erogazione del servizio ed e' associato alla RPT e alla RT al fine di qualificare in maniera univoca il versamento;
aa) prestatore dei servizi di pagamento: gli istituti di credito, Poste Italiane e gli altri soggetti che, ai sensi del decreto legislativo 27 gennaio 2010 n.11 e successive modifiche ed integrazioni, mettono a disposizione strumenti atti ad effettuare pagamenti.

Capo II

SISTEMI INFORMATICI DEL DOMINIO GIUSTIZIA

Art. 3
Funzionamento dei sistemi del dominio giustizia

1. I sistemi del dominio giustizia sono strutturati in conformità al codice dell'amministrazione digitale, alle disposizioni del Codice in materia di protezione dei dati personali e in particolare alle prescrizioni in materia di sicurezza dei dati, nonché al decreto ministeriale emanato a norma dell'articolo 1, comma 1, lettera f), del decreto del Ministro della giustizia 27 marzo 2000, n. 264.
2. Il responsabile per i sistemi informativi automatizzati del Ministero della giustizia è responsabile dello sviluppo, del funzionamento e della gestione dei sistemi informatici del dominio giustizia.
3. I dati sono custoditi in infrastrutture informatiche di livello distrettuale o interdistrettuale, secondo le specifiche di cui all'articolo 34.

Art. 4
Gestore della posta elettronica certificata del Ministero della giustizia

1. Salvo quanto previsto all'articolo 19, il Ministero della giustizia si avvale di un proprio servizio di posta elettronica certificata conforme a quanto previsto dal codice dell'amministrazione digitale.
2. Gli indirizzi di posta elettronica certificata degli uffici giudiziari e degli UNEP, da utilizzare unicamente per i servizi dicui al presente decreto, sono pubblicati sul portale dei servizi telematici e rispettano le specifiche tecniche stabilite ai sensi dell'articolo 34.
3. Il Ministero della giustizia garantisce la conservazione dei log dei messaggi transitati attraverso il proprio gestore di posta elettronica certificata per cinque anni.

Art. 5
Gestore dei servizi telematici

1. Il gestore dei servizi telematici assicura l'interoperabilita' tra i sistemi informatici utilizzati dai soggetti abilitati interni, il portale dei servizi telematici e il gestore di posta elettronica certificata del Ministero della giustizia.

Art. 6
Portale dei servizi telematici

1. Il portale dei servizi telematici consente l'accesso da parte dell'utente privato alle informazioni, ai dati e ai provvedimenti giudiziari secondo quanto previsto dall'articolo 51 del codice in materia di protezione dei dati personali.
2. L'accesso di cui al comma 1 avviene a norma dell'articolo 64 del codice dell'amministrazione digitale e secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
3. Il portale dei servizi telematici mette a disposizione dei soggetti abilitati esterni i servizi di consultazione, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
4. Il portale dei servizi telematici mette a disposizione i servizi di pagamento telematico, secondo quanto previsto dal capo V del presente decreto.
5. Il portale dei servizi telematici mette a disposizione dei soggetti abilitati e degli utenti privati, in un'apposita area, i documenti che contengono dati sensibili oppure che eccedono le dimensioni del messaggio di posta elettronica certificata di cui all'articolo 13, comma 8, secondo le specifiche

tecniche stabilite ai sensi dell'articolo 34 e nel rispetto dei requisiti di sicurezza di cui all'articolo 26.
6. Il portale dei servizi telematici consente accesso senza l'impiego di apposite credenziali, sistemi di identificazione e requisiti di legittimazione, alle informazioni ed alla documentazione sui servizi telematici del dominio giustizia, alle raccolte giurisprudenziali e alle informazioni essenziali sullo stato dei procedimenti pendenti, che vengono rese disponibili in forma anonima.

Art. 7
Registro generale degli indirizzi elettronici

1. Il registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia, contiene i dati identificativi e l'indirizzo di posta elettronica certificata dei soggetti abilitati esterni di cui al comma 3 e degli utenti privati di cui al comma 4.
2. Per i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato, il registro generale degli indirizzi elettronici e' costituito mediante i dati contenuti negli elenchi riservati di cui all'articolo 16, comma 7, del Decreto-legge 29 novembre 2008, n. 185, convertito nella legge del 28 gennaio 2009 n. 2, inviati al Ministero della giustizia secondo le specifiche tecniche di cui all'articolo 34.
3. Per i soggetti abilitati esterni non iscritti negli albi di cui al comma 2, il registro generale degli indirizzi elettronici e' costituito secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
4. Per le persone fisiche, quali utenti privati, che non operano nelle qualità di cui ai commi 2 e 3, gli indirizzi sono consultabili ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei Ministri 6 maggio 2009, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
5. Per le imprese, gli indirizzi sono consultabili, senza oneri, ai sensi dell'articolo 16, comma 6, del decreto-legge 29 novembre 2008, n. 185, convertito nella legge del 28 gennaio 2009 n. 2, con le modalità di cui al comma 10 del medesimo articolo e secondo le specifiche tecniche di cui all'articolo 34.
6. Il registro generale degli indirizzi elettronici è accessibile ai soggetti abilitati mediante le specifiche tecniche stabilite ai sensi dell'articolo 34.

Art. 8
Sistemi informatici per i soggetti abilitati interni

1. I sistemi informatici del dominio giustizia mettono a disposizione dei soggetti abilitati interni le funzioni di ricezione, accettazione e trasmissione dei dati e dei documenti informatici nonché di consultazione e gestione del fascicolo informatico, secondo le specifiche di cui all'articolo 34.
2. L'accesso dei soggetti abilitati interni è effettuato con le modalità definite dalle specifiche tecniche di cui all'articolo 34, che consentono l'accesso anche dall'esterno del dominio giustizia.
3. Nelle specifiche di cui al comma 2 sono disciplinati i requisiti di legittimazione e le credenziali di accesso al sistema da parte delle strutture e dei soggetti abilitati interni.

Art. 9
Sistema informatico di gestione del fascicolo informatico

1. Il Ministero della giustizia gestisce i procedimenti utilizzando le tecnologie dell'informazione e della comunicazione, raccogliendo in un fascicolo informatico gli atti, i documenti, gli allegati, le ricevute di posta elettronica certificata e i dati del procedimento medesimo da chiunque formati, ovvero le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo.

2. Il sistema di gestione del fascicolo informatico è la parte del sistema documentale del Ministero della giustizia dedicata all'archiviazione e al reperimento di tutti i documenti informatici, prodotti sia all'interno che all'esterno, secondo le specifiche tecniche di cui all'articolo 34.
3. La tenuta e conservazione del fascicolo informatico equivale alla tenuta e conservazione del fascicolo d'ufficio su supporto cartaceo, fermi restando gli obblighi di conservazione dei documenti originali unici su supporto cartaceo previsti dal codice dell'amministrazione digitale e dalla disciplina processuale vigente.
4. Il fascicolo informatico reca l'indicazione:
a) dell'ufficio titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
b) dell'oggetto del procedimento;
c) dell'elenco dei documenti contenuti.
5. Il fascicolo informatico è formato in modo da garantire la facile reperibilità ed il collegamento degli atti ivi contenuti in relazione alla data di deposito, al loro contenuto, ed alle finalità dei singoli documenti.
6. Con le specifiche tecniche di cui all'articolo 34 sono definite le modalità per il salvataggio dei log relativi alle operazioni di accesso al fascicolo informatico.

Art. 10
Infrastruttura di comunicazione

1. I sistemi informatici del dominio giustizia utilizzano l'infrastruttura tecnologica resa disponibile nell'ambito del Sistema Pubblico di Connettività per le comunicazioni con l'esterno del dominio giustizia.

Capo III
TRASMISSIONE DI ATTI E DOCUMENTI INFORMATICI

Art. 11
Formato dell'atto del processo in forma di documento informatico

1. L'atto del processo in forma di documento informatico è privo di elementi attivi ed è redatto nei formati previsti dalle specifiche tecniche di cui all'articolo 34; le informazioni strutturate sono in formato XML, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, pubblicate sul portale dei servizi telematici.
2. La nota di iscrizione a ruolo può essere trasmessa per via telematica come documento informatico sottoscritto con firma digitale; le relative informazioni sono contenute nelle informazioni strutturate di cui al primo comma, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

Art. 12
Formato dei documenti informatici allegati

1. I documenti informatici allegati all'atto del processo sono privi di elementi attivi e hanno i formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34.
2. E' consentito l'utilizzo dei formati compressi, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, purché contenenti solo file nei formati previsti dal comma precedente.

Art. 13

Trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati

1. I documenti informatici di cui agli articoli 11 e 12 sono trasmessi da parte dei soggetti abilitati esterni e degli utenti privati mediante l'indirizzo di posta elettronica certificata risultante dal registro generale degli indirizzi elettronici, all'indirizzo di posta elettronica certificata dell'ufficio destinatario, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. I documenti informatici di cui al comma 1 si intendono ricevuti dal dominio giustizia nel momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del Ministero della giustizia.
3. Nel caso previsto dal comma 2 la ricevuta di avvenuta consegna attesta, altresì, l'avvenuto deposito dell'atto o del documento presso l'ufficio giudiziario competente.
Quando la ricevuta è rilasciata dopo le ore 14 il deposito si considera effettuato il giorno feriale immediatamente successivo.
4. Il rigetto del deposito da parte dell'ufficio non impedisce il successivo deposito entro i termini assegnati o previsti dalla vigente normativa processuale.
5. La certificazione dei professionisti abilitati e dei soggetti abilitati esterni pubblici è effettuata dal gestore dei servizi telematici sulla base dei dati presenti nel registro generale degli indirizzi elettronici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
6. Al fine di garantire la riservatezza dei documenti da trasmettere, il soggetto abilitato esterno utilizza un meccanismo di crittografia, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
7. Il gestore dei servizi telematici restituisce al mittente l'esito dei controlli effettuati dal dominio giustizia nonché dagli operatori della cancelleria o della segreteria, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
8. La dimensione massima del messaggio è stabilita nelle specifiche tecniche di cui all'articolo 34. Se il messaggio eccede tale dimensione, il gestore dei servizi telematici genera e invia automaticamente al mittente un messaggio di errore, contenente l'avviso del rifiuto del messaggio, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
9. I soggetti abilitati esterni possono avvalersi dei servizi del punto di accesso, di cui all'articolo 23, per la trasmissione dei documenti; in tale caso il punto di accesso si attiene alle modalità di trasmissione dei documenti di cui al presente articolo.

Art. 14
Documenti probatori e allegati non informatici

1. I documenti probatori e gli allegati depositati in formato non elettronico sono identificati e descritti in una apposita sezione delle informazioni strutturate di cui all'articolo 11, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. La cancelleria o la segreteria dell'ufficio giudiziario provvede ad effettuare copia informatica dei documenti probatori e degli allegati su supporto cartaceo e ad inserirla nel fascicolo informatico, apponendo la firma digitale ai sensi e per gli effetti di cui all'articolo 22, comma 3 del codice dell'amministrazione digitale.

Art. 15
Deposito dell'atto del processo da parte dei soggetti abilitati interni

1. L'atto del processo, redatto in formato elettronico da un soggetto abilitato interno e sottoscritto con firma digitale, è depositato telematicamente nel fascicolo informatico.

2. In caso di atto formato da organo collegiale l'originale del provvedimento è sottoscritto con firma digitale anche dal presidente.
3. Quando l'atto è redatto dal cancelliere o dal segretario dell'ufficio giudiziario questi vi appone la propria firma digitale e ne effettua il deposito nel fascicolo informatico.
4. Se il provvedimento del magistrato è in formato cartaceo, il cancelliere o il segretario dell'ufficio giudiziario ne estrae copia informatica nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34 e provvede a depositarlo nel fascicolo informatico, apponendovi la propria firma digitale.

Art. 16
Comunicazioni per via telematica

1. La comunicazione per via telematica dall'ufficio giudiziario ad un soggetto abilitato esterno o all'utente privato avviene mediante invio di un messaggio dall'indirizzo di posta elettronica certificata dell'ufficio giudiziario mittente all'indirizzo di posta elettronica certificata del destinatario, indicato nel registro generale degli indirizzi elettronici, ovvero per la persona fisica consultabile ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 e per l'impresa indicato nel registro delle imprese, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. La cancelleria o la segreteria dell'ufficio giudiziario provvede ad effettuare una copia informatica dei documenti cartacei da comunicare nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34, che conserva nel fascicolo informatico.
3. La comunicazione per via telematica si intende perfezionata nel momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del destinatario e produce gli effetti di cui agli articoli 45 e 48 del codice dell'amministrazione digitale.
4. Fermo quanto previsto dall'articolo 20, comma 6, e salvo il caso fortuito o la forza maggiore, negli uffici giudiziari individuati con il decreto di cui all'articolo 51, comma 2, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, nel caso in cui viene generato un avviso di mancata consegna previsto dalle regole tecniche della posta elettronica certificata, si procede ai sensi del comma 3 del medesimo articolo 51 e viene pubblicato nel portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, un apposito avviso di avvenuta comunicazione o notificazione dell'atto nella cancelleria o segreteria dell'ufficio giudiziario, contenente i soli elementi identificativi del procedimento e delle parti e loro patrocinatori. Tale avviso è visibile solo dai soggetti abilitati esterni legittimati ai sensi dell'articolo 27, comma 1, del decreto ministeriale 21 febbraio 2011 n. 44.
5. Le ricevute di avvenuta consegna e gli avvisi di mancata consegna vengono conservati nel fascicolo informatico.
6. La comunicazione che contiene dati sensibili è effettuata per estratto con contestuale messa a disposizione dell'atto integrale nell'apposita area del portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34 e nel rispetto dei requisiti di sicurezza di cui all'articolo 26, con modalità tali da garantire l'identificazione dell'autore dell'accesso e la tracciabilità delle relative attività.
7. Nel caso previsto dal comma 6, si applicano le disposizioni di cui ai commi 2 e 3, ma la comunicazione si intende perfezionata il giorno feriale successivo al momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del destinatario.
8. Si applica, in ogni caso, il disposto dell'articolo 49 del codice dell'amministrazione digitale.

Art. 17
Notificazioni per via telematica

1. Al di fuori dei casi previsti dall'articolo 51, del decreto legge 25 giugno 2008 n. 112, convertito con modificazioni dalla legge 6 agosto 2008, n. 133, e successive modificazioni, le richieste telematiche di un'attività di notificazione da parte di un ufficio giudiziario sono inoltrate al sistema informatico dell'UNEP, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. Le richieste di altri soggetti sono inoltrate all'UNEP tramite posta elettronica certificata, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
3. La notificazione per via telematica da parte dell'UNEP rispetta i requisiti richiesti per la comunicazione da un ufficio giudiziario verso i soggetti abilitati esterni di cui all'articolo 16.
4. Il sistema informatico dell'UNEP individua l'indirizzo di posta elettronica del destinatario dal registro generale degli indirizzi elettronici, dal registro delle imprese o dagli albi o elenchi costituiti ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008, n. 185 convertito con modificazioni dalla legge 28 gennaio 2009, n. 2, nonché per il cittadino dall'elenco reso consultabile ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 in base alle specifiche tecniche stabilite ai sensi dell'articolo 34.
5. Il sistema informatico dell'UNEP, eseguita la notificazione, trasmette per via telematica a chi ha richiesto il servizio il documento informatico con la relazione di notificazione sottoscritta mediante firma digitale e congiunta all'atto cui si riferisce, nonché le ricevute di posta elettronica certificata, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
6. L'ufficiale giudiziario, se non procede alla notificazione per via telematica, effettua la copia cartacea del documento informatico, attestandone la conformità all'originale, e provvede a notificare la copia stessa con le modalità previste dalla normativa processuale vigente.

Art. 18
Notificazioni per via telematica eseguite dagli avvocati

1. L'avvocato che procede alla notificazione con modalità telematica ai sensi dell'articolo 3-bis della legge 21 gennaio 1994, n. 53, allega al messaggio di posta elettronica certificata documenti informatici o copie informatiche, anche per immagine, di documenti analogici privi di elementi attivi e redatti nei formati consentiti dalle specifiche tecniche stabilite ai sensi dell'articolo 34.
2. Quando il difensore procede alla notificazione delle comparse o delle memorie, ai sensi dell'articolo 170, quarto comma, del codice di procedura civile, la notificazione è effettuata mediante invio della memoria o della comparsa alle parti costituite ai sensi del comma 1.
3. La parte rimasta contumace ha diritto a prendere visione degli atti del procedimento tramite accesso al portale dei servizi telematici e, nei casi previsti, anche tramite il punto di accesso.
4. L'avvocato che estrae copia informatica per immagine dell'atto formato su supporto analogico, compie l'asseverazione prevista dall'articolo 22, comma 2, del codice dell'amministrazione digitale, inserendo la dichiarazione di conformità all'originale nella relazione di notificazione, a norma dell'articolo 3-bis, comma 5, della legge 21 gennaio 1994, n. 53.
5. La procura alle liti si considera apposta in calce all'atto cui si riferisce quando è rilasciata su documento informatico separato allegato al messaggio di posta elettronica certificata mediante il quale l'atto è notificato. La disposizione di cui al periodo precedente si applica anche quando la procura alle liti è rilasciata su foglio separato del quale è estratta copia informatica, anche per immagine.

6. La ricevuta di avvenuta consegna prevista dall'articolo 3-bis, comma 3, della legge 21 gennaio 1994, n. 53 è quella completa, di cui all'articolo 6, comma 4, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.».

Art. 19
Disposizioni particolari per la fase delle indagini preliminari

1. Nelle indagini preliminari le comunicazioni tra l'ufficio del pubblico ministero e gli ufficiali ed agenti di polizia giudiziaria avvengono su canale sicuro protetto da un meccanismo di crittografia secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. Le specifiche tecniche assicurano l'identificazione dell'autore dell'accesso e la tracciabilità delle relative attività, anche mediante l'utilizzo di misure di sicurezza ulteriori rispetto a quelle previste dal disciplinare tecnico di cui all'allegato B del codice in materia di protezione dei dati personali.
3. Per le comunicazioni di atti e documenti del procedimento di cui al comma 1 sono utilizzati i gestori di posta elettronica certificata delle forze di polizia. Gli indirizzi di posta elettronica certificata sono resi disponibili unicamente agli utenti abilitati sulla base delle specifiche stabilite ai sensi dell'articolo 34.
4. Alle comunicazioni previste dal presente articolo si applicano, in quanto compatibili, le disposizioni dell'articolo 16, commi 1, 2, 3, 4 e 5, e dell'articolo 20.
5. L'atto del processo in forma di documento informatico è privo di elementi attivi ed è redatto dalle forze di polizia nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34; le informazioni strutturate sono in formato XML, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34. L'atto del processo, protetto da meccanismi di crittografia, è sottoscritto con firma digitale. Si applicano, in quanto compatibili, l'articolo 14 del presente decreto, nonché gli articoli 20 e 21 del codice dell'amministrazione digitale.
6. La comunicazione degli atti del processo alle forze di polizia, successivamente al deposito previsto dall'articolo 15, è effettuata per estratto con contestuale messa a disposizione dell'atto integrale, protetto da meccanismo di crittografia, in apposita area riservata all'interno del dominio giustizia, accessibile solo dagli appartenenti alle forze di polizia legittimati, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34 e nel rispetto dei requisiti di sicurezza di cui all'articolo 26.
7. Per la gestione del fascicolo informatico si applicano, in quanto compatibili, le disposizioni di cui all'articolo 9, commi da 1 a 5. Agli atti contenuti nel fascicolo informatico, custodito in una sezione distinta del sistema documentale di cui all'articolo 9, protetta da un meccanismo di crittografia secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, hanno accesso unicamente i soggetti abilitati interni appositamente abilitati. Alla conclusione delle indagini preliminari, e in ogni altro caso in cui il fascicolo o parte di esso deve essere consultato da soggetti abilitati esterni o da utenti privati, questi accedono alla copia resa disponibile mediante il punto di accesso e il portale dei servizi telematici, secondo quanto
previsto al capo IV.
8. Per la trasmissione telematica dei flussi informativi sintetici delle notizie di reato e dei relativi esiti tra il Centro Elaborazione Dati del Servizio per il Sistema Informativo Interforze, di cui all'articolo 8, della legge 1° aprile 1981, n. 121 e successive modifiche ed integrazioni, e il sistema dei registri delle notizie di reato delle Procure della Repubblica sono utilizzate le infrastrutture di connettività delle pubbliche amministrazioni che consentono una interconnessione tra le Amministrazioni, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34. Il canale di comunicazione è protetto con le modalità di cui al comma 1.

9. Per assicurare la massima riservatezza della fase delle indagini preliminari la base di dati dei registri di cui al comma 8 è custodita, con le speciali misure di cui al comma 2, separatamente rispetto a quella relativa ai procedimenti per i quali è stato emesso uno degli atti di cui all'articolo 60, del codice di procedura penale, in infrastrutture informatiche di livello distrettuale o interdistrettuale individuate dal responsabile per i sistemi informativi automatizzati. I compiti di vigilanza sulle procedure di sicurezza adottate sulla base dati prevista dal presente comma sono svolti dal Procuratore della Repubblica presso il Tribunale e dal Procuratore generale della Repubblica presso la Corte di appello competenti in relazione all'ufficio giudiziario titolare dei dati, avvalendosi del personale tecnico individuato dal responsabile per i sistemi informativi automatizzati.

Art. 20
Requisiti della casella di PEC del soggetto abilitato esterno

1. Il gestore di posta elettronica certificata del soggetto abilitato esterno, fermi restando gli obblighi previsti dal decreto del Presidente della Repubblica 11 febbraio 2005, n.68 e dal decreto ministeriale 2 novembre 2005, recante «Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata», è tenuto ad adottare software antispam idoneo a prevenire la trasmissione di messaggi di posta elettronica indesiderati.
2. Il soggetto abilitato esterno è tenuto a dotare il terminale informatico utilizzato di software idoneo a verificare l'assenza di virus informatici per ogni messaggio in arrivo e in partenza e di software antispam idoneo a prevenire la trasmissione di messaggi di posta elettronica indesiderati.
3. Il soggetto abilitato esterno è tenuto a conservare, con ogni mezzo idoneo, le ricevute di avvenuta consegna dei messaggi trasmessi al dominio giustizia.
4. La casella di posta elettronica certificata deve disporre di uno spazio disco minimo definito nelle specifiche tecniche di cui all'articolo 34.
5. Il soggetto abilitato esterno è tenuto a dotarsi di servizio automatico di avviso dell'imminente saturazione della propria casella di posta elettronica certificata e a verificare la effettiva disponibilità dello spazio disco a disposizione.
6. La modifica dell'indirizzo elettronico può avvenire dall'1 al 31 gennaio e dall'1 al 31 luglio.
7. La disposizione di cui al comma 6 non si applica qualora la modifica dell'indirizzo si renda necessaria per cessazione dell'attività da parte del gestore di posta elettronica certificata.

Art. 21
Richiesta delle copie di atti e documenti

1. Il rilascio della copia di atti e documenti del processo avviene, previa verifica del regolare pagamento dei diritti previsti, tramite invio all'indirizzo di posta elettronica certificata del richiedente, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. L'atto o il documento che contiene dati sensibili o di grandi dimensioni è messo a disposizione nell'apposita area del portale dei servizi telematici, nel rispetto dei requisiti di sicurezza stabiliti ai sensi dell'articolo 34.
3. Nel caso di richiesta di copia informatica, anche parziale, conforme al documento originale in formato cartaceo, il cancelliere ne attesta la conformità all'originale sottoscrivendola con la propria firma digitale.

Capo IV
CONSULTAZIONE DELLE INFORMAZIONI DEL DOMINIO GIUSTIZIA

Art. 22
Servizi di consultazione

1. Ai fini di cui agli articoli 50, comma 1, 52 e 56 del codice dell'amministrazione digitale, l'accesso ai servizi di consultazione delle informazioni rese disponibili dal dominio giustizia avviene tramite un punto di accesso o tramite il portale dei servizi telematici, nel rispetto dei requisiti di sicurezza di cui all'articolo 26.

Art. 23
Punto di accesso

1. Il punto di accesso può essere attivato esclusivamente dai soggetti indicati dai commi 6 e 7.
2. Il punto di accesso fornisce un'adeguata qualità dei servizi, dei processi informatici e dei relativi prodotti, idonea a garantire la sicurezza del sistema, nel rispetto dei requisiti tecnici di cui all'articolo 26.
3. Il punto di accesso fornisce adeguati servizi di formazione e assistenza ai propri utenti, anche relativamente ai profili tecnici.
4. La violazione da parte del gestore di un punto di accesso dei livelli di sicurezza e di servizio comporta la sospensione dell'autorizzazione ad erogare i servizi fino al ripristino di tali livelli.
5. Il Ministero della giustizia dispone ispezioni tecniche, anche a campione, per verificare l'attuazione delle prescrizioni di sicurezza.
6. Possono gestire uno o più punti di accesso:
a) i consigli degli ordini professionali, i collegi ed i Consigli nazionali professionali, limitatamente ai propri iscritti;
b) il Consiglio nazionale forense, ove delegato da uno o più consigli degli ordini degli avvocati, limitatamente agli iscritti del consiglio delegante;
c) il Consiglio nazionale del notariato, limitatamente ai propri iscritti;
d) l'Avvocatura dello Stato, le amministrazioni statali o equiparate, e gli enti pubblici, limitatamente ai loro iscritti e dipendenti;
e) le Regioni, le città metropolitane, le provincie ed i Comuni, o enti consorziati tra gli stessi.
f) Le Camere di Commercio, per le imprese iscritte nel relativo registro.
7. I punti di accesso possono essere altresì gestiti da società di capitali in possesso di un capitale sociale interamente versato non inferiore a un milione di euro.

Art. 24
Elenco pubblico dei punti di accesso

1. L'elenco pubblico dei punti di accesso attivi presso il Ministero della giustizia comprende le seguenti informazioni:
a) identificativo del punto di accesso;
b) sede legale del soggetto titolare del punto di accesso;
c) indirizzo internet;
d) dati relativi al legale rappresentante del punto di accesso o a un suo delegato, comprendenti: nome, cognome, codice fiscale, indirizzo di posta elettronica certificata, numero di telefono e di fax;
e) recapiti relativi ai referenti tecnici da contattare in caso di problemi.

Art. 25
Iscrizione nell'elenco pubblico dei punti di accesso

1. Il soggetto che intende costituire un punto di accesso inoltra domanda di iscrizione nell'elenco pubblico dei punti di accesso secondo il modello e con le modalità stabilite dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia con apposito decreto, da adottarsi entro sessanta giorni dall'entrata in vigore del presente decreto.
2. Il Ministero della giustizia decide sulla domanda entro trenta giorni, con provvedimento motivato, anche sulla base di apposite verifiche, effettuabili anche da personale esterno all'Amministrazione, da questa delegato, con costi a carico del richiedente.
3. Con il provvedimento di cui al comma 2, il Ministero della giustizia delega la responsabilità del processo di identificazione dei soggetti abilitati esterni al punto di accesso. Il Ministero della giustizia può delegare la responsabilità del processo di identificazione degli utenti privati agli enti pubblici di cui all'articolo 23, comma 6, lettera e).
4. Il Ministero della giustizia può verificare l'adempimento degli obblighi assunti da parte del gestore del punto di accesso di propria iniziativa oppure su segnalazione. In caso di violazione si applicano le disposizioni di cui all'articolo 23, comma 3.

Art. 26
Requisiti di sicurezza

1. L'accesso ai servizi di consultazione delle informazioni rese disponibili dal dominio giustizia avviene mediante identificazione sul punto di accesso o sul portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
2. Il punto di accesso stabilisce la connessione con il portale dei servizi telematici mediante un collegamento sicuro con mutua autenticazione secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
3. A seguito dell'identificazione viene in ogni caso trasmesso al gestore dei servizi telematici il codice fiscale del soggetto che effettua l'accesso.
4. I punti di accesso garantiscono un'adeguata sicurezza del sistema con le modalità tecniche specificate in un apposito piano depositato unitamente all'istanza di cui all'articolo 25, a pena di inammissibilità della stessa.

Art. 27
Visibilità delle informazioni

1. Ad eccezione della fase di cui all'articolo 19, il dominio giustizia consente al soggetto abilitato esterno l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui è costituito o svolge attività di esperto o ausiliario. L'utente privato accede alle informazioni contenute nei fascicoli dei procedimenti in cui è parte mediante il portale dei servizi telematici e, nei casi previsti dall'articolo 23, comma 6, lettere e) ed f), e comma 7, mediante il punto di accesso.
2. E' sempre consentito l'accesso alle informazioni necessarie per la costituzione o l'intervento in giudizio in modo tale da garantire la riservatezza dei nomi delle parti e limitatamente ai dati identificativi del procedimento.
3. In caso di delega, rilasciata ai sensi dell'articolo 9 regio decreto legge 27 novembre 1933, n. 1578, il dominio giustizia consente l'accesso alle informazioni contenute nei fascicoli dei procedimenti patrocinati dal delegante, previa comunicazione, a cura di parte, di copia della

delega stessa al responsabile dell'ufficio giudiziario, che provvede ai conseguenti adempimenti. L'accesso è consentito fino alla comunicazione della revoca della delega.
4. La delega, sottoscritta con firma digitale, è rilasciata in conformità alle specifiche di strutturazione di cui all'articolo 35, comma 4.
5. Gli esperti e gli ausiliari del giudice accedono ai servizi di consultazione nel limite dell'incarico ricevuto e della autorizzazione concessa dal giudice.
6. Salvo quanto previsto dal comma 2, gli avvocati e i procuratori dello Stato accedono alle informazioni contenute nei fascicoli dei procedimenti in cui è parte una pubblica amministrazione la cui difesa in giudizio è stata assunta dal soggetto che effettua l'accesso.

Art. 28
Registrazione dei soggetti abilitati esterni e degli utenti privati

1. L'accesso ai servizi di consultazione resi disponibili dal dominio giustizia si ottiene previa registrazione presso il punto di accesso autorizzato o presso il portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, comma 1.
2. I punti di accesso trasmettono al Ministero della giustizia le informazioni relative ad i propri utenti registrati, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, comma 1.

Art. 29
Orario di disponibilità dei servizi di consultazione

1. Il portale dei servizi telematici e il gestore dei servizi telematici garantiscono la disponibilità dei servizi secondo le specifiche tecniche stabilite ai sensi dell'articolo 34. In ogni caso è garantita la disponibilità dei servizi di consultazione nei giorni feriali dalle ore otto alle ore ventidue, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentun dicembre.

Capo V
PAGAMENTI TELEMATICI

Art. 30
Pagamenti

1. Il pagamento del contributo unificato e degli altri diritti e spese è effettuato nelle forme previste dal decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni. La ricevuta e la attestazione di pagamento o versamento è allegata alla nota di iscrizione a ruolo o ad altra istanza inviata all'ufficio, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, ed è conservata dall'interessato per essere esibita a richiesta dell'ufficio.
2. Il pagamento di cui al comma 1 può essere effettuato per via telematica con le modalità e gli strumenti previsti dal decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni e dalle altre disposizioni normative e regolamentari relative al riversamento delle entrate alla Tesoreria dello Stato.
3. L'interazione tra le procedure di pagamento telematico messe a disposizione dal prestatore del servizio di pagamento, il punto di accesso e il portale dei servizi telematici avviene su canale sicuro, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
4. Il processo di pagamento telematico assicura l'univocità del pagamento mediante l'utilizzo della richiesta di pagamento telematico (RPT), della ricevuta telematica (RT) e dell'identificativo univoco

di erogazione del servizio (CRS) che impediscono, mediante l'annullamento del CRS, un secondo utilizzo della RT. Le specifiche tecniche sono definite ai sensi dell'articolo 34.
5. La ricevuta telematica, firmata digitalmente dal prestatore del servizio di pagamento che effettua la riscossione o da un soggetto da questo delegato, costituisce prova del pagamento alla Tesoreria dello Stato ed è conservata nel fascicolo informatico.
6. L'ufficio verifica periodicamente con modalità telematiche la regolarità delle ricevute o attestazioni e il buon esito delle transazioni di pagamento telematico.

Art. 31
Diritto di copia

1. L'interessato, all'atto della richiesta di copia, richiede l'indicazione dell'importo del diritto corrispondente che gli è comunicato senza ritardo con mezzi telematici dall'ufficio, secondo le specifiche stabilite ai sensi dell'articolo 34.
2. Alla richiesta di copia è associato un identificativo univoco che, in caso di pagamento dei diritti di copia non contestuale, viene evidenziato nel sistema informatico per consentire il versamento secondo le modalità previste dal decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni.
3. La ricevuta telematica è associata all'identificativo univoco.

Art. 32
Registrazione, trascrizione e voltura degli atti

1. La registrazione, la trascrizione e la voltura degli atti avvengono in via telematica nelle forme previste dall'articolo 73 del decreto del Presidente della Repubblica 30 maggio 2002, n.115, e successive modificazioni.

Art. 33
Pagamento dei diritti di notifica

1. Il pagamento dei diritti di notifica viene effettuato nelle forme previste dall'articolo 30.
2. L'UNEP rende pubblici gli importi dovuti a titolo di anticipazione. Eseguita la notificazione, l'UNEP comunica l'importo definitivo e restituisce il documento informatico notificato previo versamento del conguaglio dovuto dalla parte oppure unitamente al rimborso del maggior importo versato in acconto.

Capo VI
DISPOSIZIONI FINALI E TRANSITORIE
Art. 34
Specifiche tecniche

1. Le specifiche tecniche sono stabilite dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia, sentito DigitPA e, limitatamente ai profili inerenti alla protezione dei dati personali, sentito il Garante per la protezione dei dati personali.
2. Le specifiche di cui al comma precedente vengono rese disponibili mediante pubblicazione nell'area pubblica del portale dei servizi telematici.
3. Fino all'emanazione delle specifiche tecniche di cui al comma 1, continuano ad applicarsi, in quanto compatibili, le disposizioni anteriormente vigenti.

Art. 35
Disposizioni finali e transitorie

1. L'attivazione della trasmissione dei documenti informatici da parte dei soggetti abilitati esterni è preceduta da un decreto dirigenziale che accerta l'installazione e l'idoneità delle attrezzature informatiche, unitamente alla funzionalità dei servizi di comunicazione dei documenti informatici nel singolo ufficio.
2. L'indirizzo elettronico già previsto dal decreto del Ministro della Giustizia, 17 luglio 2008 recante «Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile» è utilizzabile per un periodo transitorio non superiore a sei mesi dalla data di entrata in vigore del presente decreto.
3. La data di attivazione dell'indirizzo di posta elettronica certificata di cui all'articolo 4, comma 2, e' stabilita, per ciascun ufficio giudiziario, con apposito decreto dirigenziale del responsabile per i sistemi informativi automatizzati del Ministero della giustizia che attesta la funzionalità del sistema di posta elettronica certificata del Ministero della giustizia.
4. Le caratteristiche specifiche della strutturazione dei modelli informatici sono definite con decreto del responsabile per i sistemi informativi automatizzati del Ministero della giustizia e pubblicate nell'area pubblica del portale dei servizi telematici.
5. Fino all'emanazione dei provvedimenti di cui al comma 4, conservano efficacia le caratteristiche di strutturazione dei modelli informatici di cui al decreto del Ministro della giustizia 10 luglio 2009, recante "Nuova strutturazione dei modelli informatici relativa all'uso di strumenti informatici e telematici nel processo civile e introduzione dei modelli informatici per l'uso di strumenti informatici e telematici nelle procedure esecutive individuali e concorsuali", pubblicato nella Gazzetta Ufficiale n. 165 del 18 luglio 2009 - s. o. n. 120.

Art. 36
Adeguamento delle regole tecnico-operative

1. Le regole tecnico-operative sono adeguate all'evoluzione scientifica e tecnologica, con cadenza almeno biennale, a decorrere dalla data di entrata in vigore del presente decreto.

Art. 37
Efficacia

1. Il presente decreto acquista efficacia il trentesimo giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.
2. Dalla data di cui al comma 1, cessano di avere efficacia nel processo civile le disposizioni del decreto del Presidente della Repubblica 13 febbraio 2001, n. 123 e del decreto del Ministro della giustizia 17 luglio 2008.
Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Roma, 21 febbraio 2011

Il Ministro della giustizia: Alfano
Il Ministro per la pubblica amministrazione e l'innovazione: Brunetta

Visto, il Guardasigilli: Alfano
Registrato alla Corte dei conti l'11 aprile 2011
Ministeri istituzionali, registro n. 8, foglio n. 84

16.3. Le specifiche tecniche del 18 luglio 2011

PROVVEDIMENTO 18 luglio 2011

Pubblicato per estratto sulla Gazzetta Ufficiale n. 175 del 29-7-2011 e in forma integrale sul sito internet istituzionale del Ministero della giustizia, www.giustizia.it al seguente indirizzo:
http://www.giustizia.it/giustizia/it/mg_1_8_1.wp?previsiousPage=mg_1_8&contentId=SDC656178
nonché nell'area pubblica del portale dei servizi telematici www.processotelematico.giustizia.it
recante
« Specifiche tecniche previste dall'articolo 34, comma 1 del decreto del Ministro della giustizia in data 21 febbraio 2011 n. 44, recante 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. »

Ministero della Giustizia
Direzione generale per i sistemi informativi automatizzati
Il responsabile per i sistemi informativi automatizzati
VISTO il decreto del Ministro della giustizia in data 21 febbraio 2011, n. 44 (pubblicato sulla Gazzetta Ufficiale n. 89 del 18 aprile 2011), portante “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;
VISTO il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni;
VISTO il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in mate-ria di protezione dei dati personali» e successive modificazioni;
VISTO il decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, re-cante «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della L. 16 gennaio 2003, n. 3»;
VISTO il decreto ministeriale 27 aprile 2009 recante «Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia»;
VISTO il decreto del presidente del consiglio dei ministri 6 maggio 2009, recante «Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini»;
RILEVATA la necessità di adottare le specifiche tecniche previste dall’articolo 34, comma 1, del citato decreto ministeriale 21 febbraio 2011, n. 44;
ACQUISITO il parere espresso in data 17 giugno 2011 dal Garante per la protezione dei dati personali;
ACQUISITO il parere espresso in data 15 giugno 2011 da DigitPA;

EMANA
IL SEGUENTE PROVVEDIMENTO:

CAPO I – PRINCIPI GENERALI

ART. 1
(Ambito di applicazione)

1. Il presente provvedimento stabilisce le specifiche tecniche previste dall'articolo 34, comma 1, del 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.

ART. 2
(Definizioni)

1. Ai fini del presente provvedimento, oltre alle definizioni contenute nell'articolo 2 del regolamento, si intende:
a) regolamento: il decreto del Ministro della giustizia in data 21 febbraio 2011, n. 44, portante "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;
b) CEC-PAC: Comunicazione Elettronica Certificata tra Pubblica Amministrazione e Cittadini, di cui al D.P.C.M. 6 maggio 2009;
c) CNS: Carta Nazionale dei Servizi;
d) CSV: Comma-separated values;
e) DTD: Document Type Definition;
f) D.G.S.I.A.: Direzione Generale per i Sistemi Informativi Automatizzati del Ministero della Giustizia, responsabile per i sistemi informativi automatizzati;
g) GSU: Sistema di gestione informatizzata dei registri per gli uffici notifiche e protesti;
h) HSM: Hardware Security Module;
i) HTTPS: HyperText Transfer Protocol over Secure Socket Layer;
j) IMAP: Internet Message Access Protocol;
k) PdA: Punto di Accesso, come definito all'art. 23 del regolamento;
l) PEC: Posta Elettronica Certificata;
m) POP: Post Office Protocol;
n) PP.AA.: Pubbliche Amministrazioni;
o) RdA: Ricevuta di Accettazione della Posta Elettronica Certificata;
p) RdAC: Ricevuta di Avvenuta Consegna della Posta Elettronica Certificata;
q) ReGIndE: Registro Generale degli Indirizzi Elettronici, come definito all'art. 7 del regolamento;
r) SMTP: Simple Mail Transfer Protocol;
s) UU.GG.: Uffici Giudiziari;
t) WSDL: Web Services Definition Language;
u) XML; eXtensible Markup Language;
v) XSD: XML Schema Definition;
w) SPC: Sistema Pubblico di Connettività;

x) PKCS#11: interfaccia di programmazione che consente di accedere alle funzionalità crittografiche del token; tramite l'opportuna sequenza di chiamate al token per mezzo dell'interfaccia PKCS#11 è possibile implementare la procedura di identificazione.
y) CAdES (CMS Advanced Electronic Signature): formato di busta crittografica definito nella norma ETSI TS 101 733 V1.7.4 e basata a sua volta sulle specifiche RFC 3852 e RFC 2634 e successive modificazioni.
z) PAdES (PDF Advanced Electronic Signature): formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modificazioni.
aa) OID (Object IDentifier): codice univoco basato su una sequenza ordinata di numeri per l'identificazione di evidenze informatiche utilizzate per la rappresentazione di oggetti come estensioni, attributi, documenti e strutture di dati in genere nell'ambito degli standard internazionali relativi alla interconnessione dei sistemi aperti che richiedono un'identificazione univoca in ambito mondiale.

CAPO II – SISTEMI INFORMATICI DEL DOMINIO GIUSTIZIA

ART. 3
(Infrastrutture informatiche – art. 3 del regolamento)

1) Il sistema informatico del Ministero della giustizia è articolato, salvo le infrastrutture unitarie e comuni, a livello interdistrettuale e distrettuale. In fase transitoria e quando ragioni tecniche lo rendono assolutamente necessario, possono essere mantenute strutture a livello locale.
2) Fermo quanto previsto da altre disposizioni, costituiscono infrastrutture unitarie e comuni le banche dati e i sistemi informatici indicati nell'allegato 1.
3) Il sistema di posta elettronica certificata è gestito dal fornitore presso la propria sala server, collegata ad SPC secondo le relative regole di interoperabilità e sicurezza.
4) Il dispiegamento di detti sistemi rispetta le disposizioni di cui al decreto del Ministro della giustizia in data 27 aprile 2009, recante "Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia".
5) Il Responsabile S.I.A. emana ed aggiorna periodicamente, con proprio decreto, le linee guida per la organizzazione e gestione del sistema informatico, sentito il Garante per la protezione dei dati personali. Le linee guida sono rese note con gli opportuni strumenti di comunicazione ed in ogni caso sul sito internet dell'Amministrazione.
6) Le strutture elaborative serventi ed i dati sono allocati in corrispondenza delle componenti di cui ai commi precedenti.

ART. 4
(Gestore della posta elettronica certificata del Ministero della giustizia – art. 4 del regolamento)

1. Il Ministero della giustizia si avvale del proprio gestore di posta elettronica certificata, che rilascia e gestisce apposite caselle di PEC degli uffici giudiziari e degli UNEP da utilizzare esclusivamente per i servizi previsti dal regolamento, nel rispetto delle specifiche tecniche riportate in questo provvedimento.
2. Le caselle appartengono ad apposito sotto-dominio (civile.ptel.giustiziacert.it e penale.ptel.giustiziacert.it) e possono ricevere unicamente messaggi di posta elettronica certificata. I messaggi di posta elettronica ordinaria vengono automaticamente scartati.
3. Il gestore dei servizi telematici utilizza i protocolli POP3, POP3S, IMAP, IMAPS e SMTP per collegarsi al gestore di posta elettronica certificata del Ministero.

4. La codifica dei singoli uffici, comprensiva del relativo indirizzo di PEC, è contenuta nel catalogo dei servizi telematici di cui all'articolo 5, comma 3.
5. Non possono essere utilizzate diverse caselle di PEC per la trasmissione e il deposito di atti processuali.
6. Il Ministero della giustizia conserva il log dei messaggi, transitati attraverso il proprio gestore di posta elettronica certificata, per dieci anni. A tal fine, il gestore di PEC del Ministero invia giornalmente, a una casella di posta di sistema, il log in formato CSV. Il log, sottoscritto con firma digitale o firma elettronica qualificata, è relativo a tutti gli indirizzi del sotto-dominio delle caselle del processo telematico e contiene tutti gli eventi relativi ai messaggi pervenuti, conservando le seguenti informazioni:
a) il codice identificativo univoco assegnato al messaggio originale;
b) la data e l'ora dell'evento;
c) il mittente del messaggio originale;
d) i destinatari del messaggio originale;
e) l'oggetto del messaggio originale;
f) il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.);
g) il codice identificativo dei messaggi correlati generati (ricevute, errori, ecc.);
h) il gestore mittente.
7. Un apposito modulo nell'ambito del portale dei servizi telematici comprende i componenti funzionali necessari per l'acquisizione, il salvataggio e l'interrogazione dei log prodotti dal servizio di PEC.
8. I web service d'interrogazione dei log PEC sono disponibili ai sistemi interni al dominio Giustizia.
9. Le comunicazioni di atti e documenti tra l'ufficio del pubblico ministero e gli ufficiali ed agenti di polizia giudiziaria nella fase delle indagini preliminari, avvengono mediante i gestori di posta elettronica certificata delle forze di polizia, le cui caselle sono rese disponibili unicamente agli utenti abilitati; in questo caso il gestore dei servizi telematici utilizza un canale sicuro progetto da un meccanismo di crittografia ai sensi di quanto previsto dall'articolo 20.

ART. 5
(Portale dei servizi telematici – art. 6 del regolamento)

1. Il portale dei servizi telematici è accessibile all'indirizzo www.processotelematico.giustizia.it ed è composto di una "area pubblica" e di una "area riservata".
2. L'"area pubblica", dal titolo "Servizi online Uffici Giudiziari", è composta da tutte le pagine web e i servizi del portale disponibili ad accesso senza l'impiego di apposite credenziali, sistemi di identificazione e requisiti di legittimazione; in essa sono disponibili le seguenti tipologie d'informazione:
a) Informazioni e documentazione sui servizi telematici del dominio giustizia;
b) Raccolte giurisprudenziali;
c) Informazioni essenziali sullo stato dei procedimenti pendenti, rese disponibili in forma anonima; in questo caso, i parametri e i risultati di ricerca riportano unicamente i dati identificativi dei procedimenti (numero di ruolo, numero di sentenza, ecc.), senza riferimenti in chiaro ai nomi o ai dati personali delle parti e tali per cui non sia possibile risalire all'identità dell'interessato. Il canale di comunicazione per l'accesso a tali informazioni è cifrato (HTTPS).
3. Nell'area pubblica è consultabile il catalogo dei servizi telematici, che si compone di una serie di file aventi lo scopo di censire, in forma strutturata, tutte le informazioni relative ai servizi telematici, secondo gli XSD di cui all'Allegato 10.

4. Per “area riservata” s’intende il contenitore di tutte le pagine e i servizi del portale disponibili previa identificazione informatica, come disciplinata dall’articolo 6.
5. Nell’area riservata sono disponibili informazioni, dati e provvedimenti giudiziari in formato elettronico, secondo quanto previsto all’art. 27 del regolamento, nonché i servizi di pagamento telematico e di richiesta copie.

ART. 6
(Identificazione informatica – art. 6 del regolamento)

1. L’identificazione informatica avviene sul portale dei servizi telematici mediante carta d'identità elettronica o carta nazionale dei servizi e sul punto di accesso mediante token crittografico (smart card, chiavetta USB o altro dispositivo sicuro); in quest’ultimo caso, l’identificazione avviene nel rispetto dei seguenti requisiti:
a) Il certificato deve essere rilasciato da una Certification Authority (CA), accreditata da DigitPA, che si fa garante dell’identità del soggetto.
b) Il certificato deve rispettare il profilo del certificato previsto dalla Carta Nazionale dei Servizi (CNS), facendo riferimento all’Appendice 1 del documento rilasciato dal CNIPA: “Linee guida per l’emissione e l’utilizzo della Carta Nazionale dei Servizi”. L’estensione Certificate Policy (2.5.29.32) può essere valorizzata con un Object Identifier (OID) definito dalla CA.
c) In termini di sicurezza, i dispositivi ammessi sono i dispositivi personali consentiti per la firma elettronica qualificata e quindi smart card e to-ken USB, secondo quanto previsto dalla normativa vigente. I dispositivi sicuri devono essere certificati Common Criteria EAL4+ con traguardo di sicurezza o profilo di protezione conforme alle disposizioni comunitarie.
d) In termini d’interoperabilità, sono ammissibili dispositivi che consentano la disponibilità di entrambe le interfacce PKCS#11 e CSP; in particolare entrambe le interfacce devono consentire l’accesso alla procedura d’identificazione forte mediante digitazione del PIN da parte dell’utente; il dispositivo deve inoltre rispettare la strutturazione del file system come da specifiche CNS.
2. In fase di identificazione, il punto di accesso o il portale dei servizi telematici verifica la validità del certificato presente nel token crittografico utilizzato dall’utente che accede; prima di consentire qualunque operazione, inoltre, il punto di accesso verifica che il token crittografico sia collegato alla postazione; in caso contrario, invalida e termina la sessione.
3. Il Ministero della giustizia verifica, anche attraverso opportune visite ispettive, che i punti di accesso rispettino i predetti requisiti.
4. La violazione di queste regole di sicurezza comporta per il punto di accesso la sospensione dell’autorizzazione a erogare i servizi, fino al definitivo rispetto dei requisiti.
5. Possono essere utilizzati certificati di autenticazione non conformi alle specifiche di cui sopra, purché emessi entro il 30 settembre 2011.

ART. 7
(Registro generale degli indirizzi elettronici – art. 7 del regolamento)

1. Il Registro Generale degli Indirizzi Elettronici (ReGIndE) è gestito dal Ministero della giustizia e contiene i dati identificativi nonché l’indirizzo di PEC dei soggetti abilitati esterni.
2. Il ReGIndE censisce i soggetti abilitati esterni che intendono fruire dei servizi telematici di cui al presente regolamento.
3. I sistemi di gestione informatizzata dei registri di cancelleria utilizzano il ReGIndE al fine di evitare l’inserimento manuale dei dati.

4. Le categorie di soggetti (nel prosieguo anche enti) il cui profilo anagrafico alimenta il ReGIndE sono:
a) soggetti appartenenti ad un ente pubblico che svolgano uno specifico ruolo nell'ambito di procedimenti (ad esempio avvocati e funzionari dell'INPS e dell'Avvocatura dello Stato, avvocati e funzionari delle PP.AA.);
b) professionisti iscritti in albi ed elenchi istituiti con legge (ad esempio consiglio dell'ordine degli avvocati o consiglio nazionale del Notariato);
c) professionisti non iscritti ad alcun albo: tutti quei soggetti nominati dal giudice come consulenti tecnici d'ufficio – o più in generale ausiliari del giudice – non appartenenti ad un ordine di categoria o che appartengono ad ente/ordine professionale che non abbia ancora inviato l'albo al Ministero della giustizia (ad eccezione degli avvocati).
5. Il ReGIndE non gestisce informazioni già presenti in registri disponibili alle PP.AA., qualora questi siano accessibili in via telematica ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008 n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009 n. 2, il cui contenuto occorre ai sistemi del dominio Giustizia; da tali registri (tra cui il registro delle imprese, delle pubbliche amministrazioni e dei cittadini) sono recuperati gli indirizzi di PEC dei professionisti e delle imprese, nonché gli indirizzi CEC-PAC dei cittadini ivi censiti.
6. Il ReGIndE è direttamente accessibile dai sistemi interni al dominio giustizia, attraverso un apposito web service.
7. Il ReGIndE è consultabile dai soggetti abilitati esterni tramite il proprio punto di accesso o tramite il Portale dei Servizi Telematici (area riservata), su connessioni sicure (SSL v3), attraverso un apposito web service; i relati-vi WSDL sono pubblicati nell'area pubblica del portale dei servizi telematici.

ART. 8
(Alimentazione del registro generale degli indirizzi elettronici – art. 7 del regolamento)

1. L'alimentazione del ReGIndE avviene previo invio al responsabile per i sistemi informativi automatizzati di un documento di censimento contenente le informazioni necessarie ad identificare:
a) l'ente stesso attraverso: codice ente, descrizione, codice fiscale/partita iva;
b) il nominativo e il codice fiscale del delegato all'invio dell'albo, che dovrà sottoscrivere con firma digitale o firma elettronica qualificata l'albo in trasmissione;
c) la casella di PEC utilizzata per l'invio dell'albo.
2. Il documento di censimento di cui al comma precedente aderisce al modello reperibile nell'area pubblica del portale e viene inviato all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati: prot.dgsia.dog@giustiziacert.it.
3. Terminate le operazioni di censimento da parte del responsabile per i sistemi informativi automatizzati, l'ente mittente del documento di censimento riceve una risposta; in caso di esito positivo, l'ente può procedere all'invio dell'albo secondo le seguenti specifiche:
a) il messaggio deve essere di posta elettronica certificata; non sono considerati i messaggi di posta ordinaria;
b) non vi sono vincoli sull'oggetto né sul body del messaggio;
c) l'indirizzo di PEC mittente deve essere censito tra quelli delegati all'invio e riportati nel documento di censimento;
d) deve essere allegato un solo file (ComunicazioniSoggetti.xml), sottoscritto con firma digitale o firma elettronica qualificata;

e) la firma digitale o firma elettronica qualificata deve appartenere al soggetto delegato di cui al comma 1, lettera b, sulla base del codice fiscale censito;
f) il file ComunicazioniSoggetti.xml deve essere conforme all'XML-Schema di cui all'Allegato 2;
g) il codice ente specificato nel file deve essere tra quelli censiti.
4. Il mancato rispetto di uno o più dei vincoli di cui all'articolo precedente comporta un messaggio automatico di esito negativo; in questo caso l'allegato ComunicazioniSoggetti.xml viene scartato.
5. A ogni invio corrisponde una risposta tramite PEC; il messaggio ha come oggetto la medesima descrizione del messaggio originale con il suffisso "– Esito" e riporta in allegato l'esito dell'elaborazione del messaggio con le eventuali eccezioni; il formato del messaggio di esito, inviato come allegato al messaggio di PEC, è descritto nell'Allegato 3.
6. L'esito si riferisce sia ad errori presenti sui dati e, quindi riconducibili alle informazioni dei singoli soggetti (come ad esempio codice fiscale inesistente), sia ad errori legati a vincoli e prerequisiti che presuppongono la validità dell'invio di un albo (ad esempio: censimento dell'ente richiedente e dei soggetti abilitati all'invio dell'albo).
7. Ad ogni nuovo indirizzo di PEC registrato nelle anagrafiche a seguito dell'inserimento di un nuovo soggetto o di modifica di uno esistente, viene inviato un messaggio di PEC di cortesia in cui si attesta l'avvenuta registrazione.

ART. 9
(Professionisti non iscritti in albi – art. 7 del regolamento)

1. I professionisti non iscritti all'albo, oppure per i quali il proprio ordine di appartenenza non abbia provveduto all'invio di copia dell'albo (ad eccezione degli avvocati), si registrano al ReGIndE attraverso un Punto di Accesso (PdA) o attraverso il Portale dei Servizi Telematici, previa identificazione, effettuando altresì l'inserimento (upload) del file che contiene copia informatica, in formato PDF, dell'incarico di nomina da parte del giudice; tale file è sottoscritto con firma digitale o firma elettronica qualificata dal soggetto che intende iscriversi.
2. Il PdA provvede a trasmettere l'avvenuta registrazione con le medesime modalità di cui all'articolo precedente, con la differenza che il file ComunicazioniSoggetti.xml è digitalmente sottoscritto con firma digitale o firma elettronica qualificata dal PdA.
3. Qualora il professionista di cui al comma 1 s'iscriva ad un albo, oppure pervenga copia dell'albo da parte dell'ordine di appartenenza, prevalgono i dati trasmessi dall'ordine stesso; in questo caso il sistema cancella la prima iscrizione e invia un messaggio PEC di cortesia al professionista.

ART. 10
(Sistemi informatici per i soggetti abilitati interni – art. 8 del regolamento)

1. I sistemi informatici a disposizione dei soggetti abilitati interni sono conformi alle regole di cui al D.M. 27 aprile 2009 e mettono a disposizione le funzioni relative a:
a) ricezione, accettazione e trasmissione dei dati e dei documenti informatici;
b) consultazione e gestione del fascicolo informatico.
2. Per l'accesso ai sistemi di cui al comma precedente dall'interno degli uffici giudiziari, l'identificazione è effettuata mediante coppia di credenziali "nome utente/password" ovvero mediante identificazione informatica ai sensi dell'articolo 6.
3. Per l'accesso ai sistemi di cui al comma 1 dall'esterno della Rete Giustizia, l'identificazione è effettuata dal portale dei servizi telematici sulla base del sistema "Active Directory Nazionale" (ADN) e secondo le specifiche di cui all'articolo 6; ai soli fini del recupero dall'esterno delle informazioni di registro da parte dei sistemi a disposizione dei magistrati in ambito civile, è

sufficiente l'identificazione sulla base del sistema ADN purché l'interrogazione dei dati finalizzati al recupero preveda l'indicazione del numero di ruolo generale nonché del codice fiscale dell'attore principale e del convenuto principale del procedimento.

ART. 11
(Fascicolo informatico – art. 9 del regolamento)

1. Il fascicolo informatico raccoglie i documenti (atti, allegati, ricevute di posta elettronica certificata) da chiunque formati, nonché le copie informatiche dei documenti; raccoglie altresì le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo.
2. Il sistema di gestione del fascicolo informatico, realizzato secondo quanto previsto all'articolo 41 del CAD, è la parte del sistema documentale del Ministero della giustizia che si occupa di archiviare e reperire tutti i documenti informatici, prodotti sia all'interno che all'esterno; fornisce pertanto ai sistemi fruitori (sistemi di gestione dei registri di cancelleria, gestore dei servizi telematici e strumenti a disposizione dei magistrati) tutte le primitive – esposte attraverso appositi web service – necessarie per il recupero, l'archiviazione e la conservazione dei documenti informatici, secondo le normative in vigore; l'accesso al sistema di gestione documentale avviene soltanto per il tramite dei sistemi fruitori, che gestiscono le logiche di profilazione e autorizzazione.
3. Le operazioni di accesso al fascicolo informatico sono registrate in un apposito file di log che contiene le seguenti informazioni:
a) il codice fiscale del soggetto che ha effettuato l'accesso;
b) il riferimento al documento prelevato o consultato (codice identificativo del documento nell'ambito del sistema documentale);
c) la data e l'ora dell'accesso.
Il suddetto file di log è sottoposto a procedura di conservazione, sempre nell'ambito del sistema documentale, per cinque anni.

CAPO III
TRASMISSIONE DI ATTI E DOCUMENTI INFORMATICI
ART. 12
(Formato dell'atto del processo in forma di documento informatico – art. 11 del regolamento)

1. L'atto del processo in forma di documento informatico rispetta i seguenti requisiti:
a) è in formato PDF;
b) è privo di elementi attivi;
c) è ottenuto da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è pertanto ammessa la scansione di immagini;
d) è sottoscritto con firma digitale o firma elettronica qualificata esterna, pertanto il file ha la seguente denominazione: <nome file libero>.pdf.p7m;
e) è corredato da un file in formato XML, che contiene le informazioni strutturate nonché tutte le informazioni della nota di iscrizione a ruolo, e che rispetta gli XSD riportati nell'Allegato 5; esso è denominato DatiAtto.xml ed è sottoscritto con firma digitale o firma elettronica qualificata.
2. La struttura del documento firmato è CAdES; il certificato di firma è inserito nella busta crittografica La modalità di apposizione della firma digitale o della firma elettronica qualificata è del tipo "firme multiple indipendenti" o parallele , e prevede che uno o più soggetti firmino, ognuno con la propria chiave privata, lo stesso documento (o contenuto della busta). L'ordine di apposizione delle firme dei firmatari non è significativo e un'alterazione dell'ordinamento delle firme non pregiudica la validità della busta crittografica; il file generato si presenta con un'unica

estensione p7m. Il meccanismo qui descritto è valido sia per l'apposizione di una firma singola che per l'apposizione di firme multiple.

ART. 13
(Formato dei documenti informatici allegati – art. 12 del regolamento)

1. I documenti informatici allegati sono privi di elementi attivi, tra cui macro e campi variabili, e sono consentiti nei seguenti formati:
a) .pdf
b) .odf
c) .rtf
d) .txt
e) .jpg
f) .gif
g) .tiff
h) .xml.
2. È consentito l'utilizzo dei seguenti formati compressi purché contenenti file nei formati previsti al comma precedente:
a) .zip
b) .rar
c) .arj.

3. Gli allegati possono essere sottoscritta con firma digitale o firma elettronica qualificata; nel caso di formati compressi la firma digitale, se presente, deve essere applicata dopo la compressione.

ART. 14
(Trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati – art. 13 del regolamento)

1. L'atto e gli allegati sono contenuti nella cosiddetta "busta telematica", ossia un file in formato MIME che riporta tutti i dati necessari per l'elaborazione da parte del sistema ricevente (gestore dei servizi telematici); in particolare la busta contiene il file Atto.enc, ottenuto dalla cifratura del file Atto.msg, il quale contiene a sua volta:
a) IndiceBusta.xml: il DTD è riportato nell'Allegato 4.
b) DatiAtto.xml: gli XSD sono riportati nell'Allegato 5.
c) <nome file (libero)>.pdf.p7m: atto vero e proprio, in formato PDF, sottoscritto con firma digitale o firma elettronica qualificata (firma esterna).
d) AllegatoX.xxx[.p7m]: uno o più allegati nei formati di file di cui all'articolo 13, eventualmente sottoscritti con firma digitale o firma elettronica qualificata; il nome del file può essere scelto liberamente.
2. La cifratura di Atto.msg è eseguita con la chiave di sessione (ChiaveSessione) cifrata con il certificato del destinatario; IssuerDname è il Distinguished Name della CA che ha emesso il certificato dell'ufficio giudiziario o dell'UNEP destinatario, SerialNumber è il numero seriale del certificato dell'ufficio giudiziario o dell'UNEP destinatario; l'algoritmo utilizzato per l'operazione di cifratura simmetrica del file è il 3DES e le chiavi simmetriche di sessione sono cifrate utilizzando la chiave pubblica contenuta nel certificato del destinatario; le chiavi di cifratura degli uffici giudiziari sono disponibili nell'area pubblica del portale dei servizi telematici (il relativo percorso e nome file è indicato nel catalogo dei servizi telematici); lo standard previsto è il CAdES.

3. La dimensione massima consentita per la busta telematica è pari a 30 Me-gabyte.
4. La busta telematica viene trasmessa all'ufficio giudiziario destinatario in allegato ad un messaggio di posta elettronica certificata che rispetta le specifiche su mittente, destinatario, oggetto, corpo e allegati come riportate nell'Allegato 6.
5. Il gestore dei servizi telematici scarica il messaggio dal gestore della posta elettronica certificata del Ministero della giustizia ed effettua le verifiche formali sul messaggio; le eccezioni gestite sono le seguenti:
a) T001: l'indirizzo del mittente non è censito in ReGIndE;
b) T002: Il formato del messaggio non è aderente alle specifiche;
c) T003: la dimensione del messaggio eccede la dimensione massima consentita.
6. Il gestore dei servizi telematici, nel caso in cui il mittente sia un avvocato, effettua l'operazione di certificazione, ossia recupera lo status del difensore da ReGIndE; nel caso in cui lo status non sia "attivo", viene segnalato alla cancelleria.
7. Il gestore dei servizi telematici effettua i controlli automatici (formali) sulla busta telematica; le possibili anomalie all'esito dell'elaborazione della busta telematica sono codificate secondo le seguenti tipologie:
a) WARN: anomalia non bloccante; si tratta in sostanza di segnalazioni, tipicamente di carattere giuridico (ad esempio manca la procura alle liti allegata all'atto introduttivo);
b) ERROR: anomalia bloccante, ma lasciata alla determinazione dell'ufficio ricevente, che può decidere di intervenire forzando l'accettazione o rifiutando il deposito (esempio: certificato di firma non valido o mittente non firmatario dell'atto);
c) FATAL: eccezione non gestita o non gestibile (esempio: impossibile decifrare la busta depositata o elementi della busta mancanti ma fonda-mentali per l'elaborazione).
8. La codifica puntuale degli errori indicati al comma precedente è pubblicata e aggiornata nell'area pubblica del portale dei servizi telematici.
9. All'esito dei controlli di cui ai commi precedenti, il gestore dei servizi telematici invia al depositante un messaggio di posta elettronica certificata riportante eventuali eccezioni riscontrate.
10. Il gestore dei servizi telematici, all'esito dell'intervento dell'ufficio, invia al depositante un messaggio di posta elettronica certificata contenente l'esito dell'intervento di accettazione operato dalla cancelleria o dalla segreteria dell'ufficio giudiziario destinatario.

ART. 15
(Documenti probatori e allegati non informatici – art. 14 del regolamento)

1. I documenti probatori e gli allegati depositati in formato analogico, sono identificati e descritti in un'apposita sezione dell'atto del processo in forma di documento informatico e comprendono, per l'individuazione dell'atto di riferimento, i seguenti dati:
a) numero di ruolo della causa;
b) progressivo dell'allegato;
c) indicazione della prima udienza successiva al deposito.

ART. 16
(Deposito dell'atto del processo da parte dei soggetti abilitati interni – art. 15 del regolamento)

1. I soggetti abilitati interni utilizzano appositi strumenti per la redazione degli atti del processo in forma di documento informatico e per la loro trasmissione alla cancelleria o alla segreteria dell'ufficio giudiziario.

2. L'atto è inserito nella medesima busta telematica di cui all'articolo 14 e viene trasmesso su canale sicuro (SSL v3) al gestore dei servizi telematici, tramite collegamento sincrono (http/SOAP); si applicano le disposizioni di cui all'articolo 10, comma 2.
3. Se il provvedimento del magistrato è in formato cartaceo, il cancelliere o il segretario dell'ufficio giudiziario ne estrae copia informatica in formato PDF, e lo sottoscrive con firma digitale o firma elettronica qualificata.

ART. 17
(Comunicazioni per via telematica – art. 16 del regolamento)

1. Il gestore dei servizi telematici provvede ad inviare le comunicazioni per via telematica, provenienti dall'ufficio giudiziario, alla casella di posta elettronica certificata del soggetto abilitato esterno destinatario, recuperando il relativo indirizzo sul ReGIndE; il formato del messaggio è riportato nell'Allegato 8; la comunicazione è riportata nel corpo del messaggio nonché nel file allegato Comunicazione.xml (il relativo DTD è riportato nell'Allegato 4.
2. La cancelleria o la segreteria dell'ufficio giudiziario, attraverso apposite funzioni messe a disposizione dai sistemi informatici di cui all'articolo 10, provvede ad effettuare una copia informatica in formato PDF di eventuali documenti cartacei da comunicare; la copia informatica è conservata nel fascicolo informatico.
3. Il gestore dei servizi telematici recupera le ricevute della posta elettronica certificata e gli avvisi di mancata consegna dal gestore di PEC del Ministero e li conserva nel fascicolo informatico; la ricevuta di avvenuta consegna è di tipo breve.

ART. 18
(Comunicazioni contenenti dati sensibili – art. 16 del regolamento)

1. La comunicazione che contiene dati sensibili è effettuata per estratto: in questo caso al destinatario viene recapitato l'avviso disponibilità della comunicazione di cancelleria, secondo il formato riportato nell'Allegato 8; il destinatario effettua il prelievo dell'atto integrale accedendo all'indirizzo (URL) contenuto nel suddetto messaggio di PEC di avviso.
2. Il prelievo di cui al comma precedente avviene attraverso l'apposito servizio proxy del portale dei servizi telematici, su canale sicuro (protocollo SSL); tale servizio effettua l'identificazione informatica dell'utente, ai sensi dell'articolo 6; il prelievo è consentito unicamente se l'utente è registrato nel ReGIndE.
3. Il prelievo di cui al comma precedente avviene da un'apposita area di download del gestore dei servizi telematici, dove viene gestita e mantenuta un'apposita tabella recante le seguenti informazioni:
a) il codice fiscale del soggetto che ha effettuato il prelievo o la consulta-zione;
b) il riferimento al documento prelevato o consultato (codice univoco inserito nell'URL inviato nell'avviso di cui al comma 4);
c) la data e l'ora di invio dell'avviso;
d) la data e l'ora del prelievo o della consultazione.
4. Le informazioni di cui al comma precedente vengono conservate per cinque anni.

ART. 19
(Notificazioni per via telematica – art. 17 del regolamento)

1. Al di fuori dei casi previsti dall'articolo 51, del decreto legge 5 giugno 2008 n. 112 (convertito con modificazioni dalla legge 6 agosto 2008, n. 133) e successive modificazioni, le richieste telematiche di un'attività di notificazione da parte di un ufficio giudiziario sono inoltrate al sistema informatico dell'UNEP in formato XML, attraverso un colloquio diretto, via web service, tra i rispettivi gestori dei servizi telematici, su canale sicuro (SSL v3).
2. Le richieste di notifica effettuate dai soggetti abilitati esterni sono inoltrate all'UNEP tramite posta elettronica certificata, nel rispetto dei requisiti tecnici di cui agli articoli 12, 13 e 14; all'interno della busta telematica è inserito il file RichiestaParte.xml, il cui XML-Schema è riportato nell'Allegato 5.
3. All'UNEP può essere inviata, sempre all'interno della busta telematica, la richiesta di pignoramento il cui XML-Schema è riportato nell'Allegato 5.
4. Alla notificazione per via telematica da parte dell'UNEP si applicano le specifiche della comunicazione per via telematica di cui all'articolo 17; il formato del messaggio di posta elettronica certificata è riportato nell'Allegato 7.
5. Ai fini della notificazione per via telematica, il sistema informatico dell'UNEP recupera l'indirizzo di posta elettronica del destinatario a seconda della sua tipologia:
a) soggetti abilitati esterni e professionisti iscritti in albi o elenchi costituiti ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008, n. 185 convertito con legge del 28 gennaio 2009, n. 2: dal registro generale degli indirizzi elettronici, ai sensi dell'articolo 7, comma 6;
b) imprese iscritte nel relativo registro: ai sensi dell'articolo 7, comma 5;
c) cittadini: ai sensi dell'articolo 7, comma 5.
6. Il sistema informatico dell'UNEP, eseguita la notificazione, trasmette - per via telematica a chi ha richiesto il servizio - il documento informatico con la relazione di notificazione sottoscritta mediante firma digitale o firma elettronica qualificata e congiunta all'atto cui si riferisce, nonché le ricevute di posta elettronica certificata. La relazione di notificazione è in formato XML e rispetta l'XML-Schema riportato nell'Allegato 5; se il richiedente è un sog-getto abilitato esterno, la trasmissione avviene via posta elettronica certificata; il formato del messaggio è riportato nell'Allegato 7.

ART. 20
(Disposizioni particolari per la fase delle indagini preliminari – art. 19 del regolamento)

1. Nelle indagini preliminari le comunicazioni tra l'ufficio del pubblico ministero e gli ufficiali ed agenti di polizia giudiziaria avvengono su canale sicuro protetto da un meccanismo di crittografia (SSL v3).
2. Il sistema di gestione del registro e il sistema documentale garantiscono la tracciabilità delle attività, attraverso appositi file di log, conservati nel sistema documentale stesso.
3. L'atto del processo rispetta le specifiche di cui agli articoli 12 e 13.
4. La comunicazione di atti e documenti nella fase di indagini preliminari avviene tramite posta elettronica certificata, secondo le specifiche di cui all'articolo 17; le caselle di PEC dell'ufficio del pubblico ministero sono attivate presso i gestori di posta elettronica certificata della forze di polizia.
5. Il gestore dei servizi telematici si collega alle caselle di cui al comma precedente su canale sicuro, utilizzando i protocolli POP3Ss o HTTPS, al fine di evitare la trasmissione in chiaro delle credenziali di accesso e dei messaggi.

6. La comunicazione degli atti del processo alle forze di polizia è effettuata per estratto, secondo le specifiche di cui all'articolo 18; l'atto è protetto da meccanismo di crittografia a chiavi asimmetriche, con le medesime specifiche di cui all'articolo 14 comma 2.
7. Gli atti contenuti nel fascicolo informatico, relativi alle indagini preliminari, sono custoditi in una sezione distinta del sistema documentale; ciascun atto potrà essere protetto da un meccanismo di crittografia basato su chiavi asimmetriche, custodite e gestite nell'ambito di un sistema HSM (hardware security module) appositamente dedicato alle operazioni di cifratura e decifratura, invocato dalle applicazioni di gestione dei registri. Ogni istanza del-la piattaforma di gestione documentale è dotata di apparati HSM dedicati.
8. La trasmissione telematica delle informazioni relative alle notizie di reato avviene tramite cooperazione applicativa tra il sistema di gestione informatizzata dei registri presso l'ufficio del pubblico ministero e il Sistema Informativo Interforze del Ministero dell'Interno, secondo le specifiche del Sistema Pubblico di Cooperazione (SPCoop), su canale cifrato attraverso l'uso di certificati server. Le informazioni contenute nella busta di E-Government prevista dalle specifiche SPCoop sono in formato XML.

ART. 21
(Requisiti della casella di PEC del soggetto abilitato esterno – art. 20 del regolamento)

1. La casella di posta elettronica certificata di un soggetto abilitato esterno deve disporre di uno spazio disco minimo pari a 1 Gigabyte.

ART. 22
(Richiesta delle copie di atti e documenti – art. 21 del regolamento)

1. Per la richiesta telematica di copie di atti e documenti relativi al procedimento è disponibile, sul punto di accesso e sul portale dei servizi telematici, un servizio sincrono attraverso il quale individuare i documenti di cui richiedere copia e, in seguito al perfezionamento del pagamento, inoltrare la richiesta effettiva della copia stessa.
2. Il soggetto che ne ha diritto può richiedere:
a) copia semplice in formato digitale;
b) copia semplice per l'avvocato non costituito in formato digitale;
c) copia autentica in formato digitale;
d) copia esecutiva in formato digitale;
e) copia semplice in formato cartaceo;
f) copia autentica in formato cartaceo;
g) copia esecutiva in formato cartaceo.
3. I dati relativi alla richiesta sono inoltrati all'ufficio giudiziario attraverso l'invocazione di un apposito web service; al richiedente è restituito l'identificativo univoco della richiesta inoltrata. Tale identificativo univoco è associato all'intero flusso di gestione della richiesta e di rilascio della copia.
4. Nel caso in cui la copia non possa essere rilasciata il sistema, in maniera automatica, comunica al richiedente l'impossibilità di evadere la richiesta.

ART. 23
(Rilascio delle copie di atti e documenti – art. 21 del regolamento)

1. Il rilascio della copia in formato digitale di atti e documenti viene eseguito secondo le specifiche di cui all'articolo 16 del regolamento e dell'art. 23-ter, comma 5 del CAD; la copia è inviata al richiedente in allegato ad un messaggio di posta elettronica certificata, secondo il formato riportato nell'Allegato 9.
2. Nel caso di copia di documenti contenenti dati sensibili o nel caso di copia di documenti che eccedono il massimo consentito dalla posta elettronica certificata, il messaggio di cui al comma precedente contiene l'avviso di disponibilità della copia, secondo il formato riportato nell'Allegato 9; il prelievo avviene secondo le specifiche di cui all'articolo 18, commi 2, 3 e 4.
3. La copia, informatica o analogica, di documento informatico è corredata del contrassegno di cui all'articolo 23-ter, comma 5, del CAD, al fine di assicurare la provenienza e la conformità all'originale.
4. Il contrassegno di cui al comma precedente è generato elettronicamente su ognuna delle pagine del documento e contiene, nella forma di codice bidimensionale, la pagina del documento informatico di cui si rilascia copia sottoscritta dal cancelliere con firma digitale o firma elettronica qualificata al fine di attestarne la conformità all'originale.
5. Il contrassegno di cui al comma 3 consente la verifica automatica della conformità della copia rilasciata, qualora riprodotta a stampa, al documento informatico da cui è tratta nonché la verifica della firma digitale o firma elettronica qualificata apposta sulla copia al momento del rilascio; tale verifica può essere effettuata dal soggetto richiedente nonché dal soggetto destinatario o beneficiario dell'atto tramite un software di visualizzazione e verifica scaricabile gratuitamente dall'area pubblica del portale dei servizi telematici e configurato per riconoscere esclusivamente i contrassegni generati attraverso strumenti informatici della Giustizia.
6. Il codice bidimensionale di cui al comma 4 è generato tramite codifica Data Matrix definita nello standard ISO/IEC (16022:2006).

CAPO IV – CONSULTAZIONE DELLE INFORMAZIONI DEL DOMINIO GIUSTIZIA

ART. 24
(Requisiti di sicurezza – art. 26 del regolamento)

1. L'architettura dei servizi di consultazione aderisce al modello MVC (Model View Controller) e prevede il disaccoppiamento del front-end, localizzato sul punto di accesso o sul portale dei servizi telematici, dal back-end, localizzato sul gestore dei servizi telematici, incaricato di esporre i servizi sotto forma di web service (http/SOAP).
2. Il portale dei servizi telematici espone, attraverso un apposito servizio proxy, i web service forniti dal gestore dei servizi telematici, a beneficio dei punti di accesso e di applicazioni esterne.
3. I punti di accesso realizzano autonomamente la parte di front-end, che de-ve essere localizzata all'interno della intranet del PdA stesso e non deve es-sere accessibile direttamente dall'esterno.
4. I punti di accesso possono a loro volta esporre i web service forniti dal gestore dei servizi telematici, a beneficio di applicazioni esterne.
5. Il protocollo di trasporto tra il punto di accesso e il proxy è HTTPS; la serializzazione dei messaggi è nel formato XML/SOAP.
6. Le funzionalità fornite dai web service realizzati, nonché le relative regole di invocazione, sono descritte tramite i WSDL pubblicati sull'area pubblica del portale dei servizi telematici.
7. L'accesso ai servizi di consultazione avviene previa identificazione informatica su di un punto di accesso o sul portale dei servizi telematici, secondo le specifiche di cui all'articolo 6; a seguito di tale identificazione, il punto di accesso o il portale dei servizi telematici attribuiscono all'utente un ruolo di consultazione, a seconda del registro di cancelleria; eseguita tale operazione, viene trasmesso al proxy di cui al comma 2 il codice fiscale del soggetto che effettua l'accesso

(nell'header http) e il ruolo di consultazione stesso (nel messaggio SOAP); il proxy verifica che il soggetto sia presente nel ReGIndE e in caso trattasi di un avvocato che lo status non sia "radiato" o "cancellato"; qualora la verifica abbia esito positivo, trasmette la richiesta al web service del gestore dei servizi telematici.
8. In base al ruolo di consultazione di cui al comma precedente, il sistema fornisce le autorizzazioni all'accesso rispetto alle informazioni anagrafiche contenute nei sistemi di gestione dei registri o sulla base dell'atto di delega previsto dal regolamento.
9. In fase di richiesta di attivazione, il punto di accesso può adottare meccanismi di identificazione basati sulla gestione federata delle identità digitali (modello GFID), secondo le specifiche di DigitPA; in questo caso, il responsabile per i sistemi informativi automatizzati, valutata la soluzione proposta e opportunamente descritta nel piano della sicurezza, approva il meccanismo di identificazione che soddisfa il livello di sicurezza richiesto.
10. Fuori dai casi previsti ai commi 1 e 9, l'architettura dei servizi di consultazione prevede in via residuale che il punto di accesso o il portale dei servizi telematici effettuino, a seguito dell'identificazione di cui al comma 7, un link diretto dalle proprie pagine alla pagina principale del sito web che rende disponibili i servizi su canale sicuro (HTTPS); in questo caso i dati identificativi del soggetto vengono inseriti nell'header HTTP della richiesta.
11. I servizi di consultazione attivi sono elencati, per singolo ufficio, nel catalogo dei servizi telematici, di cui all'articolo 5, comma 5.
12. L'elenco dei punti di accesso autorizzati è pubblicato nell'area pubblica del portale dei servizi telematici e nel catalogo dei servizi telematici, di cui all'articolo 5, comma 5.
13. Il punto di accesso si dota di un piano della sicurezza, depositato al responsabile per i sistemi informativi automatizzati unitamente all'istanza di iscrizione all'elenco pubblico dei punti di accesso, che prevede la trattazione, esaustiva e dettagliata, dei seguenti argomenti:
a) struttura logistica e operativa dell'organizzazione;
b) ripartizione e definizione delle responsabilità del personale addetto;
c) descrizione dei dispositivi installati;
d) descrizione dell'infrastruttura di protezione, per ciascun immobile interessato (e rilevante ai fini della sicurezza);
e) descrizione delle procedure di registrazione delle utenze;
f) descrizione relativa all'implementazione dei meccanismi di identificazione informatica;
g) qualora il PdA integri la gestione delle caselle di PEC dei propri utenti, descrizione delle modalità di integrazione;
h) procedura di gestione delle copie di sicurezza dei dati;
i) procedura di gestione dei disastri;
j) analisi dei rischi e contromisure previste;
14. Ai fini dell'iscrizione nel suddetto elenco, il responsabile per i sistemi informativi automatizzati verifica il piano della sicurezza di cui al comma precedente e può disporre apposite verifiche in loco, in particolare per accertare il rispetto delle prescrizioni di sicurezza riportate nel presente provvedimento.
15. Il punto di accesso abilita i propri iscritti unicamente a usufruire dei servizi esplicitamente autorizzati dal responsabile per i sistemi informativi automatizzati e riportati nel catalogo dei servizi telematici.
16. Il punto di accesso si dota di una casella di posta elettronica certificata, che comunica al responsabile per i sistemi informativi automatizzati, da utilizzarsi per inviare e ricevere comunicazioni con il Ministero della Giustizia.

ART. 25

(Registrazione dei soggetti abilitati esterni e degli utenti privati – art. 28 del regolamento)

1. L'utente accede ai servizi di consultazione previa registrazione presso un punto di accesso autorizzato o presso il portale dei servizi telematici.
2. Il punto di accesso o il portale dei servizi telematici effettuano la registra-zione del soggetto abilitato esterno o dell'utente privato, prelevando il codice fiscale dal token crittografico dell'utente; attraverso un'apposita maschera web, l'utente (senza poter modificare il codice fiscale) completa i propri dati, inserendo almeno le seguenti informazioni:
a) nome e cognome
b) luogo e data di nascita
c) residenza
d) domicilio
e) ruolo
f) consiglio dell'ordine o ente di appartenenza
g) casella di posta elettronica certificata
3. I dati di cui al comma precedente, unitamente alla data in cui è avvenuta la registrazione, sono archiviati e conservati per dieci anni.
4. Gli esperti e gli ausiliari del giudice, non iscritti ad alcun albo professionale o per i quali il proprio ordine non abbia provveduto all'invio dell'albo, presentano, all'atto della registrazione, copia elettronica in formato PDF dell'incarico di nomina da parte del giudice; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che s'iscrive.
5. Qualora il professionista sia iscritto ad un albo dei consulenti tecnici, istituito presso un tribunale (ai sensi del Capo II, sezione 1, delle disposizioni di attuazione del codice di procedura civile), al PdA viene presentata copia elettronica in formato PDF del provvedimento di iscrizione all'albo stesso da parte del comitato; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che s'iscrive.
6. Il punto di accesso è tenuto a conservare i documenti informatici di cui ai commi precedenti, e a renderli disponibili, su richiesta, al Ministero della giustizia.
7. I punti di accesso trasmettono al Ministero della giustizia le informazioni relative ai propri utenti registrati secondo le modalità di cui all'allegato 11.

CAPO V – PAGAMENTI TELEMATICI

ART. 26
(Requisiti relativi al processo di pagamento telematico – art. 30 del regolamento)

1. Al fine di comunicare in via telematica all'ufficio giudiziario l'avvenuto pagamento delle spese, dei diritti e del contributo unificato, la ricevuta di versamento è inserita come allegato della busta telematica nel caso di inoltro via PEC, oppure è associata alla richiesta telematica nel caso di istanza gestita tramite un flusso sincrono.
2. Nel caso di pagamento eseguito in modalità non telematica, la ricevuta di versamento è costituita dalla copia informatica dell'originale cartaceo ottenuta per scansione e sottoscritta con firma digitale o firma elettronica qualificata da chi ne fa uso, mentre nel caso di pagamento in modalità telematica la ricevuta è costituita dal documento originale informatico in formato XML, come disciplinato all'articolo 28, comma 2.
3. Il servizio di pagamento in modalità telematica è messo a disposizione dei soggetti abilitati nell'ambito delle funzionalità del punto di accesso e del portale dei servizi telematici, con lo scopo di permettere il versamento attraverso strumenti telematici e di ricevere l'attestazione del

versamento attraverso il medesimo canale telematico; l'accesso ai servizi di pagamento avviene previa identificazione informatica di cui all'articolo 6.
4. Nell'ambito del flusso per il pagamento telematico sono individuati i seguenti componenti architetturali:
a) Sistema dei Pagamenti (SP): infrastruttura del sistema finanziario costituita dall'insieme di tutti gli strumenti con i quali possono essere acquistati beni e servizi nell'economia, nonché dalle attività e dagli intermediari che consentono l'effettivo trasferimento di tali strumenti da un operatore ad un altro;
b) Sistema del Prestatore dei servizi di Pagamento (Psp): piattaforma tecnologica operante presso gli istituti di credito, Poste Italiane o altri soggetti abilitati che, ai sensi della normativa vigente e nell'ambito del Sistema dei Pagamenti, mettono a disposizione degli utenti gli strumenti atti ad effettuare il pagamento richiesto;
c) Front-End con il Sistema dei Pagamenti (FESP): componente infrastrutturale (middleware) atto a facilitare lo scambio di informazioni tra i soggetti attraverso la condivisione dei protocolli di colloquio (sia applicativi, che di trasporto), l'implementazione delle logiche di elaborazione della richiesta di pagamento e della ricevuta telematica nonché l'erogazione di eventuali servizi aggiuntivi, tra cui la firma digitale dei documenti scambiati. Le funzioni del componente possono essere integrate in un PdA, integrate nel sistema offerto dal prestatore di servizi (Psp) o condivise (anche da più amministrazioni) essendo messe a fattor comune nell'ambito dell'infra-struttura di sistema della Pubblica Amministrazione (Nodo PA all'interno di SPC);
d) Nodo PA: infrastruttura condivisa all'interno del SPC che gestisce il colloquio con i prestatori dei servizi di pagamento (Psp) e può anche svolgere le funzioni previste per il FESP.
5. Le modalità tecniche d'interazione tra le componenti di cui al comma precedente devono essere caratterizzate dall'adozione di protocolli sicuri. Nel caso in cui l'interazione avvenga tramite la rete SPC, il requisito è garantito dalla natura riservata della rete stessa. In tutti gli altri casi, il colloquio avviene attraverso l'utilizzo di certificati "server" rilasciati da Certification Authority qualificate.
6. Le funzioni svolte dal portale dei servizi telematici integrano al loro interno le funzioni di pagamento informatico, al fine di offrire all'utente un servizio unico e completo. Le applicazioni offerte dai punti accesso si uniformano a tale principio.
7. Per dare corso al pagamento il prestatore di servizi di pagamento (Psp) concede "fiducia" all'identificazione, operata ai sensi del comma 3, dal punto di accesso o dal portale dei servizi telematici. Ai fini del completamento del processo di pagamento, il prestatore del servizio (Psp) può richiedere all'utente di autenticarsi sul proprio sistema attraverso l'immissione di ulteriori credenziali allo scopo rilasciate.
8. Il processo consente all'utente di scegliere tra diverse modalità di pagamento messe a sua disposizione da una molteplicità di prestatori di servizi di pagamento (Psp).
9. La ricevuta telematica restituita all'utente a fronte del pagamento effettuato in via telematica costituisce prova del trasferimento dell'importo versato sul conto corrente intestato alla Tesoreria dello Stato.
10. I versamenti in Tesoreria sono effettuati in modalità telematica attraverso quanto previsto dalla normativa vigente.
11. Per il recupero delle somme erroneamente versate si procede secondo le modalità previste dalla legge.

ART. 27
(Oggetti informatici interessati nel pagamento telematico – art. 30 del regolamento)

1. La Richiesta di Pagamento Telematico (RPT), relativa al versamento di una o più spettanze legate ad un medesimo servizio, è costituita da un file XML, il cui XSD è riportato nell'Allegato 5, che:
a) definisce gli elementi necessari a caratterizzare i pagamenti, in particolare qualifica il versamento con un identificativo univoco del versamento di cui al successivo comma 5;
b) contiene i dati identificativi, variabili a seconda dell'operazione per cui è richiesto il pagamento;
c) contiene una parte riservata (Dati Specifici Riscossione) per inserire informazioni elaborabili automaticamente dai sistemi della Giustizia;
d) viene predisposta dal soggetto richiedente (portale dei servizi telematici o punto di accesso) ed inviata al sistema del prestatore dei servizi di pagamento (Psp) direttamente ovvero attraverso la componente architetturale FESP;
e) può essere sottoscritta o meno con firma digitale ovvero con firma elettronica qualificata dal soggetto pagatore, a seconda degli accordi intercorsi con il Prestatore di Servizi di paga-mento (PsP).
2. La Ricevuta Telematica (RT) è predisposta dal sistema del prestatore dei servizi di pagamento (Psp) anche attraverso l'utilizzo della componente architetturale FESP ed è restituita al soggetto richiedente a fronte di ogni singola RPT: essa è costituita da un file XML, il cui XSD è riportato nell'Allegato 5, che:
a) definisce gli elementi necessari a qualificare il pagamento, tra cui l'esito del pagamento stesso e, in caso positivo, l'identificativo univoco del pagamento assegnato dal sistema del prestatore dei servizi di pagamento (Psp);
b) trasferisce inalterate le stesse informazioni ricevute in ingresso (RPT) relative alla parte riservata (Dati Specifici Riscossione) a disposizione della PA
3. Il soggetto che emette la Ricevuta Telematica (RT) di cui al comma 2, la sottoscrive- ai sensi dell'art 30, comma 5 del regolamento- con firma digitale o firma elettronica qualificata in formato CAdES; a tal fine possono essere utilizzati certificati emessi da una autorità di certificazione allo scopo messa a disposizione da DigitPA.
4. Al fine di qualificare in maniera univoca il versamento, è definito l' identificativo di erogazione del servizio (CRS) che identifica univocamente una richiesta di erogazione servizio da parte dei sistemi informatici del dominio giustizia.
5. Il CRS è generato dal portale dei servizi telematici su specifica richiesta del soggetto richiedente attraverso un servizio sincrono (tramite web service i cui WSDL sono pubblicati sull'area pubblica del portale dei servizi telematici) e ha il seguente formato: <check digits> <identificatore univoco>, dove:
a) <check digit> costituisce il codice numerico di controllo (2 posizioni);
b) <identificatore univoco> è rappresentato da 33 posizioni alfanumeriche così strutturate: <codice PdA richiedente><codice Sistema Gestore><codice univoco operazione>; la sezione <codice PdA richiedente> (4 caratteri alfanumerici) assicura flessibilità nella emissione del CRS; la sezione <codice Sistema Gestore> (4 caratteri alfanumerici) rappresenta il sistema a cui è destinata la ricevuta; la sezione <codice univoco operazione> (25 caratteri alfanumerici) contiene un codice „non ambiguo" all'interno del dominio entro il quale viene generato.
6. Il CRS viene inserito nella struttura RPT (elemento identificativoUnivoco-Versamento) e viene restituito al punto di accesso o al portale dei servizi telematici all'interno della RT (elemento identificativoUnivocoVersamento).
7. Al momento dell'accettazione della ricevuta di pagamento, il sistema informatico dell'ufficio giudiziario controlla che il CRS non sia stato già utilizzato in altre ricevute e, in tal caso, lo stesso viene annullato al fine di non permettere il riutilizzo della stessa RT.

ART. 28
(Riscontro del pagamento telematico – art. 30 del regolamento)

1. Allo scopo di permettere all'Amministrazione di verificare e riscontrare le ricevute generate a seguito di pagamento telematico, nell'ambito del dominio giustizia è configurato un sottosistema per la memorizzazione e gestione delle Ricevute Telematiche di cui all'articolo 27; il sottosistema è denominato Repository Ricevute Telematiche (RRT) ed è accessibile a tutte le applicazioni e ai sistemi del dominio Giustizia interessate dai pagamenti telematici.
2. Il punto di accesso o il portale dei servizi telematici provvede ad inviare la RT al sistema RRT contestualmente al rilascio della stessa al soggetto abilitato esterno richiedente.
3. Per l'invio della RT al Repository Ricevute Telematiche è messo a disposizione un apposto servizio (web service) esposto nell'ambito del portale dei servizi telematici; i relativi WSDL sono pubblicati nell'area pubblica del portale dei servizi telematici.
4. Il sistema RRT permette la gestione delle RT e dei relativi CRS secondo le modalità indicate nell'articolo 27.
5. Le informazioni relative ai pagamenti contenute nel sistema di cui al comma 1 sono messe a disposizione, sulla base di specifica convenzione da sottoscriversi con il responsabile per i sistemi informativi automatizzati, degli enti e delle agenzie pubbliche per l'adempimento dei propri compiti di verifica, controllo e contrasto all'evasione ed elusione.
6. I soggetti abilitati che hanno effettuato i versamenti in via informatica possono consultare sul portale dei servizi telematici, previa identificazione informatica di cui all'articolo 6, le informazioni relative ai pagamenti contenute nel sistema di cui al comma 1.

ART. 29
(Diritto di copia – art. 31 del regolamento)

1. Il sistema informatico del Ministero della giustizia comunica all'interessato l'importo da versare per i diritti di copia; tale importo è calcolato, sulla base delle vigenti disposizioni normative e regolamentari, in base alle indicazioni fornite dall'interessato al momento dell'individuazione dei documenti di cui richiedere copia. L'informazione è messa a disposizione dell'interessato attraverso il servizio di richiesta copie attivo sul punto di accesso e sul portale dei servizi telematici; unitamente all'importo dei diritti ed oneri viene comunicato all'interessato anche l'identificativo univoco associato alla richiesta, associato all'intero flusso di gestione della richiesta e rilascio della copia.
2. La richiesta di copia è soddisfatta solo dopo che è pervenuta la ricevuta di versamento di cui all'articolo 27, comma 2.

CAPO VI – DISPOSIZIONI FINALI E TRANSITORIE

ART. 30
(Gestione del transitorio – art. 35 del regolamento)

1. Al momento dell'attivazione, sul ReGIndE di cui all'articolo 7, dell'indirizzo di posta elettronica certificata del soggetto abilitato esterno, il portale dei servizi telematici invia un messaggio di PEC al medesimo soggetto comunicando l'avvenuta attivazione. La comunicazione riporta espressa avvertenza che il soggetto abilitato esterno dovrà usare per le successive trasmissioni unicamente la casella PEC.

2. Contestualmente all'invio della comunicazione di cui al comma 1, il portale invia un messaggio di PEC alla casella di servizio del PdA, prevista dall'articolo 25, comma 16.
3. A decorrere dalla comunicazione di cui al comma 1, il soggetto abilitato e-sterno utilizza unicamente il sistema di trasmissione della posta elettronica certificata, così come disciplinato nel presente provvedimento.
4. A decorrere dalla comunicazione di cui al comma 1, il gestore dei servizi telematici:
a) Invia comunicazioni e notificazioni solamente alla casella di PEC ivi indicata;
b) Consente la ricezione di atti solo tramite PEC, rifiutando automaticamente il deposito tramite altro canale.

ART. 31
(Efficacia)

1. Il presente decreto acquista efficacia decorsi 15 giorni dalla sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.
Roma, addì 18 luglio 2011
IL RESPONSABILE PER I SISTEMI INFORMATIVI AUTOMATIZZATI DEL MINISTERO DELLA GIUSTIZIA
Stefano Aprile
Ministero dell'economia e delle finanze - dipartimento della ragioneria generale dello stato ufficio centrale del bilancio presso il ministero della giustizia visto e registrato n. 11750/II
Roma, 21 luglio 2011
IL DIRIGENTE DELL'UFFICIO
Stefano Pesce
Allegati
All. 1 - Banche dati e sistemi di cui all'articolo 3, comma 2 (formato pdf, 12 Kb)
All. 2 - Struttura di ComunicazioniSoggetti.xml (formato pdf, 65 Kb)
All. 3 - Struttura di Esiti.xml (formato pdf, 40 Kb)
All. 4 - DTD dei file e messaggi di sistema (formato pdf, 15 Kb)
All. 5 - Struttura di DatiAtto.xml (formato pdf, 1236 Kb)
All. 6 - Formato dei messaggi relativi al deposito della busta telematica (formato pdf, 19 Kb)
All. 7 - Formato dei messaggi relativi alle notificazioni telematiche (formato pdf, 15 Kb)
All. 8 - Formato dei messaggi relativi alle comunicazioni telematiche (formato pdf, 24 Kb)
All. 9 - Formato dei messaggi relativi al rilascio delle copie (formato pdf, 15 Kb)
All. 10 - XSD relativi al catalogo dei servizi telematici (formato pdf, 28 Kb)
All. 11 - Informazioni sugli utenti dei punti di accesso (formato pdf, 10 Kb)

16.4 Legge 21 gennaio 1994 n. 53 (facoltà di notificazioni di atti civili, amministrativi e stragiudiziali per gli avvocati).

Legge 21 gennaio 1994, n. 53

FACOLTA' DI NOTIFICAZIONI DI ATTI CIVILI, AMMINISTRATIVI E STRAGIUDIZIALI PER GLI AVVOCATI

(così come modificata dalla Legge n. 148/2011 pubblicata nella Gazzetta Ufficiale n. 265 del 14 novembre 2011 e **dall'art. 1 comma 19 della Legge 24 dicembre 2012, n. 228 Disposizioni per la**

formazione del bilancio annuale e pluriennale dello Stato (Legge di stabilita' 2013). (GU n. 302 del 29-12-2012).

Articolo 1

1. L'avvocato o il procuratore legale, munito di procura alle liti a norma dell'articolo 83 del codice di procedura civile e della autorizzazione del consiglio dell'ordine nel cui albo è iscritto a norma dell'articolo 7 della presente legge, può eseguire la notificazione di atti in materia civile, amministrativa e stragiudiziale a mezzo del servizio postale, secondo le modalità previste dalla legge 20 novembre 1982, n. 890 ovvero a mezzo della posta elettronica certificata salvo che l'autorità giudiziaria disponga che la notifica sia eseguita personalmente.

Articolo 2

1. Per la notificazione di cui all'articolo 1, **effettuata a mezzo del servizio postale**, il notificante utilizza speciali buste e moduli per avvisi di ricevimento, di cui deve fornirsi a propria cura e spese, conformi al modello prestabilito dall'Amministrazione postale per la notifica a mezzo posta.

Articolo 3

1. Il notificante **che procede a norma dell'articolo 2 deve**:

a) scrivere la relazione di notificazione sull'originale e sulla copia dell'atto, facendo menzione dell'ufficio postale per mezzo del quale spedisce la copia al destinatario in piego raccomandato con avviso di ricevimento;
b) presentare all'ufficio postale l'originale e la copia dell'atto da notificare; l'ufficio postale appone in calce agli stessi il timbro di vidimazione, inserendo quindi la copia, o le copie, da notificare nelle buste di cui all'articolo 2, sulle quali il notificante ha preventivamente apposto le indicazioni del nome, cognome, residenza o dimora o domicilio del destinatario, con l'aggiunta di ogni particolarità idonea ad agevolarne la ricerca; sulle buste devono essere altresì apposti il numero del registro cronologico di cui all'articolo 8, la sottoscrizione ed il domicilio del notificante;
c) presentare contemporaneamente l'avviso di ricevimento compilato con le indicazioni richieste dal modello predisposto dall'Amministrazione postale, con l'aggiunta del numero di registro cronologico.
2. Per le notificazioni di atti effettuate prima dell'iscrizione a ruolo della causa o del deposito dell'atto introduttivo della procedura, l'avviso di ricevimento deve indicare come mittente la parte istante e il suo procuratore; per le notificazioni effettuate in corso di procedimento, l'avviso deve indicare anche l'ufficio giudiziario e, quando esiste, la sezione dello stesso.
3. Per il perfezionamento della notificazione e per tutto quanto non previsto dal presente articolo, si applicano, per quanto possibile, gli articoli 4 e seguenti della legge 20 novembre 1982, n. 890.

Art. 3-bis

1. La notificazione con modalità telematica si esegue a mezzo di posta elettronica certificata all'indirizzo risultante da pubblici elenchi, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. La notificazione può essere eseguita esclusivamente utilizzando un indirizzo di posta elettronica certificata del notificante risultante da pubblici elenchi.

2. Quando l'atto da notificarsi non consiste in un documento informatico, l'avvocato provvede ad estrarre copia informatica dell'atto formato su supporto analogico, attestandone la conformità all'originale a norma dell'articolo 22, comma 2, del decreto legislativo 7 marzo 2005, n. 82. La notifica si esegue mediante allegazione dell'atto da notificarsi al messaggio di posta elettronica certificata.
3. La notifica si perfeziona, per il soggetto notificante, nel momento in cui viene generata la ricevuta di accettazione prevista dall'articolo 6, comma 1, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e, per il destinatario, nel momento in cui viene generata la ricevuta di avvenuta consegna prevista dall'articolo 6, comma 2, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.
4. Il messaggio deve indicare nell'oggetto la dizione: 'notificazione ai sensi della legge n. 53 del 1994'.
5. L'avvocato redige la relazione di notificazione su documento informatico separato, sottoscritto con firma digitale ed allegato al messaggio di posta elettronica certificata. La relazione deve contenere:
a) il nome, cognome ed il codice fiscale dell'avvocato notificante;
b) gli estremi del provvedimento autorizzativo del consiglio dell'ordine nel cui albo è iscritto;
c) il nome e cognome o la denominazione e ragione sociale ed il codice fiscale della parte che ha conferito la procura alle liti;
d) il nome e cognome o la denominazione e ragione sociale del destinatario;
e) l'indirizzo di posta elettronica certificata a cui l'atto viene notificato;
f) l'indicazione dell'elenco da cui il predetto indirizzo è stato estratto;
g) l'attestazione di conformità di cui al comma 2.
6. Per le notificazioni effettuate in corso di procedimento deve, inoltre, essere indicato l'ufficio giudiziario, la sezione, il numero e l'anno di ruolo

Articolo 4

1 L'avvocato o il procuratore legale, munito della procura e dell'autorizzazione di cui all'articolo 1, può eseguire notificazioni in materia civile, amministrativa e stragiudiziale, direttamente mediante consegna di copia dell'atto nel domicilio del destinatario, nel caso in cui il destinatario sia altro avvocato o procuratore legale, che abbia la qualità di domiciliatario di una parte.
2. **La notifica può essere eseguita mediante consegna di copia dell'atto nel domicilio del destinatario se questi ed il notificante sono iscritti nello stesso albo. In tal caso l'originale e la copia dell'atto devono essere previamente vidimati e datati dal consiglio dell'ordine nel cui albo entrambi sono iscritti.**

Articolo 5

1.***** Nella notificazione di cui all'articolo 4 l'atto deve essere trasmesso a mezzo posta elettronica certificata all'indirizzo di posta elettronica certificata che il destinatario ha comunicato al proprio ordine, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici.

*******(N.B. Il comma 1 dell'art. 5 è stato formalmente abrogato, ai sensi e per gli effetti dell'art. 16 quater della legge 24 dicembre 2012 , n. 228 (legge stabilità 2013), il 24 maggio 2013 a seguito dell'entrata in vigore del Decreto Ministeriale 03 aprile 2013 n. 48, pubblicato nella Gazzetta Ufficiale del 09 maggio 2013).*

2. Quando la notificazione viene effettuata ai sensi dell'articolo 4, comma 2, l'atto deve essere consegnato nelle mani proprie del destinatario. Se la consegna non può essere fatta personalmente al destinatario, l'atto è consegnato, nel domicilio risultante al consiglio dell'ordine in cui il destinatario è iscritto, a persona addetta allo studio ovvero al servizio del destinatario.
3. Nei casi previsti dal comma 2 l'originale e la copia dell'atto notificato nonché il registro cronologico di cui all'articolo 8 sono sottoscritti dalla persona alla quale l'atto è consegnato e, quando la consegna sia effettuata a persona diversa dal destinatario, la firma deve essere seguita, su entrambi i documenti summenzionati, dalla specificazione delle generalità e della qualità rivestita dal consegnatario.

Articolo 6

1. L'avvocato o il procuratore legale, che compila **la relazione o le attestazioni di cui agli articoli 3, 3-bis e 9** o le annotazioni di cui all'articolo 5, è considerato pubblico ufficiale ad ogni effetto.
2. Il compimento di irregolarità o abusi nell'esercizio delle facoltà previste dalla presente legge costituisce grave illecito disciplinare, indipendentemente dalla responsabilità prevista da altre norme.

Articolo 7

1. L'avvocato o il procuratore legale, che intende avvalersi delle facoltà previste dalla presente legge, deve essere previamente autorizzato dal consiglio dell'ordine nel cui albo è iscritto; tale autorizzazione potrà essere concessa esclusivamente agli avvocati o procuratori legali che non abbiano procedimenti disciplinari pendenti e che non abbiano riportato la sanzione disciplinare della sospensione dall'esercizio professionale o altra più grave sanzione e dovrà essere prontamente revocata in caso di irrogazione delle dette sanzioni ovvero, anche indipendentemente dall'applicazione di sanzioni disciplinari, in tutti i casi in cui il consiglio dell'ordine, anche in via cautelare, ritenga motivatamente inopportuna la prosecuzione dell'esercizio delle facoltà previste dalla presente legge.
2. Il provvedimento di rigetto o di revoca, emesso in camera di consiglio dopo aver sentito il professionista, è impugnabile davanti al Consiglio nazionale forense nel termine di dieci giorni solo per motivi di legittimità ed è immediatamente esecutivo, indipendentemente dalla sua eventuale impugnazione.
3. In caso di revoca dell'autorizzazione, l'avvocato o il procuratore legale consegna al consiglio dell'ordine il registro di cui all'articolo 8, sul quale vengono annotati il provvedimento di revoca e l'eventuale annullamento del medesimo.
4. I provvedimenti del consiglio dell'ordine adottati ai sensi della presente legge sono resi pubblici nei modi più ampi.

Articolo 8

1. L'avvocato o il procuratore legale, che intende avvalersi delle facoltà previste dalla presente legge, deve munirsi di un apposito registro cronologico, il cui modello è stabilito con decreto del Ministro della giustizia, sentito il parere del Consiglio nazionale forense.
2. La validità del registro di cui al comma 1 è subordinata alla previa numerazione e vidimazione, in ogni mezzo foglio, da parte del presidente del consiglio dell'ordine nel cui albo il notificante è iscritto, o da un consigliere all'uopo delegato, previa l'autorizzazione di cui all'articolo 7.

3. Ogni notificazione eseguita ai sensi della presente legge è annotata dal notificante, giornalmente, sul registro cronologico, insieme alle eventuali annotazioni previste dagli articoli precedenti.
4. Il registro cronologico di cui al comma 1 può essere costituito da moduli continui vidimati uso computer.
4-bis. Le disposizioni del presente articolo non si applicano alle notifiche effettuate a mezzo posta elettronica certificata.

Articolo 9

1. Nei casi in cui il cancelliere deve prendere nota sull'originale del provvedimento dell'avvenuta notificazione di un atto di opposizione o di impugnazione, ai sensi dell'articolo 645 del codice di procedura civile e dell'articolo 123 delle disposizioni per l'attuazione, transitorie e di coordinamento del codice di procedura civile, il notificante provvede, contestualmente alla notifica, a depositare copia dell'atto notificato presso il cancelliere del giudice che ha pronunciato il provvedimento.
1-bis. Qualora non si possa procedere al deposito con modalità telematiche dell'atto notificato a norma dell'articolo 3-bis, l'avvocato estrae copia su supporto analogico del messaggio di posta elettronica certificata, dei suoi allegati e della ricevuta di accettazione e di avvenuta consegna e ne attesta la conformità ai documenti informatici da cui sono tratte ai sensi dell'articolo 23, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Articolo 10

1. Agli atti notificati ai sensi della presente legge è apposta, al momento dell'esibizione o del deposito nella relativa procedura, apposita marca, il cui modello e importo sono stabiliti con decreto del Ministro della giustizia.
Quando l'atto è notificato a norma dell'articolo 3-bis al pagamento dell'importo di cui al periodo precedente si provvede mediante sistemi telematici.
2. Per le violazioni della disposizione di cui al comma 1 si applicano le sanzioni previste per l'imposta di bollo, con le stesse modalità e procedure, in quanto applicabili.

Articolo 11

1. Le notificazioni di cui alla presente legge sono nulle e la nullità è rilevabile d'ufficio, se mancano i requisiti soggettivi ed oggettivi ivi previsti, se non sono osservate le disposizioni di cui agli articoli precedenti e, comunque, se vi è incertezza sulla persona cui è stata consegnata la copia dell'atto o sulla data della notifica.

Articolo 12

1. I decreti del Ministro della giustizia previsti agli articoli 8 e 10 sono emanati entro novanta giorni dalla pubblicazione nella Gazzetta ufficiale della presente legge.

Articolo 13

1. La presente legge entra in vigore il 1° luglio 1994, fatta eccezione per le disposizioni di cui all'articolo 12.

Capitolo XVII
Conclusioni

Mi ero posto come obiettivo quello di avvicinare il lettore ad una conoscenza di base del processo telematico al fine di facilitarne l'utilizzo cercando di spiegare, con termini semplici ma pertinenti, il significato di molte sigle e incomprensibili acronimi e di guidarlo nell'intricata selva di norme che costellano il processo telematico.
Mi auguro di non aver deluso le attese e spero che la lettura delle pagine sia risultata utile per fugare qualche dubbio o rafforzare qualche certezza.

Concludevo la prima stesura dell'eBook sul PCT pubblicato da Altalex nel gennaio 2012, con questa considerazione che io stesso non esitavo a definire "impopolare":
"Sono passati più di dieci anni da quando, per la prima volta, abbiamo sentito parlare di processo telematico ma, nonostante il tempo trascorso, per molti Uffici Giudiziari, tale modo di interpretare il processo è ancora sconosciuto.
Proprio per questo il legislatore, a mio avviso, dovrà decidere (e presto) se dare VERO impulso al processo telematico inserendo, ad esempio, una norma (simile a quella, citata nel presente lavoro, dell'art 4 della L. 24/2010) la quale preveda, a seguito del riconoscimento del valore legale di qualsiasi attività del PCT, un congruo termine (12/18 mesi) decorso il quale l'unica forma di processo sia quella telematica o se, in assenza di un simile provvedimento normativo, accontentarsi di avere un processo telematico IBRIDO essendo tale quello in cui, pur con le difficoltà evidenziate, si debba far affidamento al documento cartaceo, cosa questa a dir poco inverosimile soprattutto se si consideri che sempre più la pubblica amministrazione parla di DEMATERIALIZZAZIONE.
Pur avendo, nel mio elaborato, criticato alcune scelte e strategie, desumibili dalla lettura degli ultimi interventi normativi (D.M. 21.02.2011 e specifiche tecniche del 18 luglio 2011) non posso però negare la voglia e gli sforzi profusi dal legislatore nel corso del corrente anno volti a confermare e ribadire l'importanza dello strumento informatico nel processo. Ma questo non basta e non deve essere un punto d'arrivo.
Sono fermamente convinto che alcune decisioni, quelle più importanti e che consentirebbero la definitiva consacrazione del processo telematico in termini di diffusione negli Uffici Giudiziari, non vengano prese per motivi "politici" ossia per non creare il malcontento tra i molti, moltissimi, troppi operatori del mondo giustizia che, nonostante gli evidenti vantaggi, forse per un personale rifiuto ad acquisire minime competenze informatiche, ostacolano e quindi non favoriscono l'espandersi di tale innovazione che, dati alla mano, consentirebbe un sicuro risparmio sia di tempi che di risorse economiche.
E allora, se è vero che alcune regole del PCT devono trovare opportune modifiche al pari di quelle del codice di procedura civile che ne devono consentire un più fluido utilizzo è altrettanto vero che dovrà esserci anche un cambio di mentalità da parte di tutti coloro che, del mondo giustizia, sono i protagonisti.
Bisogna avere il coraggio di affrontare l'innovazione tecnologica, anche e soprattutto nel campo giuridico, al fine di trarre dalla stessa tutto quanto di positivo sia possibile trarre.
L'inizio della mia attività forense è coinciso con il momento in cui negli studi legali la macchina da scrivere elettronica, il cui utilizzo consentiva di visualizzare su un piccolo display il testo appena battuto e quindi di apportare eventuali correzioni prima di stamparlo, cominciava a lasciare il posto ai primi personal computer, costosissimi ed ingombranti ma che consentivano all'avvocato di dimezzare i tempi di elaborazione di un qualsiasi atto, di memorizzarlo con un nome e di richiamarlo per un suo uso successivo.

Ricordo l'emozione provata nell'utilizzare il mio primo computer, Apple, il "IIe", senza hard disk (disco rigido), con un drive nel quale, alternativamente, dovevano trovare collocazione giganteschi floppy (quelli da 5¼ pollici) nei quali erano contenuti sia i programmi che i dati, con un monitor a fosfori verdi e una stampante a 12 aghi il cui rumore, pur essendo fastidiosissimo, era (almeno per me) altrettanto affascinante.
Una delle prime cose da me realizzate… la carta intestata dello Studio che stampavo insieme al testo mentre la maggior parte dei colleghi utilizzava quella stampata in tipografia (sicuramente più professionale ma anche più costosa).
Insomma, siamo passati dal pennino e calamaio alla penna stilografica, dalla stampante ad aghi a quella a getto d'inchiostro, a quella laser per arrivare, oggi, ad avere fotocopiatrici a colori in grado di essere collegate ad un computer e utilizzate come stampanti, scanner e fax.
Abbiamo accettato e utilizzato a nostro vantaggio la tecnologia e il progresso ma adesso sembra che qualcosa impedisca di continuare a percorrere questa strada, proprio adesso che sta per condurci ad un traguardo importante: evitare il più possibile di recarsi nei Tribunali e di svolgere quasi tutte le attività di cancelleria rimanendo comodamente nel nostro Studio o di potersi trovare in altra nazione ed avere comunque la possibilità di ricevere notifiche in tempo reale e depositare i propri atti e tutto ciò disponendo di un computer e di un dispositivo di firma digitale.
Quale avvocato, avrebbe mai pensato, anni fa, di svolgere la professione telematicamente?
Nell'era della comunicazione elettronica, l'informatizzazione di una procedura complessa e gravosa come quella che caratterizza la Giustizia, deve senz'altro costituire un punto fermo per il Legislatore, al fine di abbattere i costi, facilitare il dialogo tra gli attori della scena processuale, e soprattutto ridurre i tempi della giustizia. L'informatizzazione del processo è una riforma necessaria, a patto che non si creino parallele, eccessive documentazioni cartacee.
L'opportunità del PCT è per gli avvocati una grande occasione ma al tempo stesso un grande cambiamento operativo nell'esercizio della professione. Le difficoltà iniziali dovranno essere superate tramite corsi formativi nei quali i protagonisti dovranno essere i Consigli dell'Ordine e tutti gli organismi dell'avvocatura.
L'esperienza e l'utilizzo del Polisweb non deve costituire un punto d'arrivo ma un punto da cui partire consapevoli che ciò consentirà di ridurre le file agli uffici depositi, agli uffici copie, nonché l'afflusso dell'utenza presso le cancellerie con vantaggi sia per il Tribunale, il quale potrà destinare ad altri impieghi le risorse umane ed economiche, sia per gli avvocati che potranno evitare file e perdite di tempo connesse al deposito o alla consultazione del fascicolo in cancelleria.
Nulla ad oggi si dice a proposito del processo verbale, relativamente alle modalità attraverso le quali poter arrivare al suo inserimento nel fascicolo informatico e che, nell'ottica del processo telematico, dovrebbero essere quelle di una redazione del verbale in maniera informatica, sottoscritto poi, con firma digitale; ciò consentirebbe di trovare nel fascicolo informatico anche il verbale di udienza consentendo quindi di estendere i vantaggi sopra evidenziati.
In mancanza di una modifica decisa delle norme che regolano il processo telematico non posso non concludere questa considerazione con una certezza: nel processo telematico sarà ancora elevato (prevalente) l'utilizzo del supporto cartaceo e fin quando la realtà sarà questa non potremo dire di avere un VERO PROCESSO TELEMATICO!
Concludo trascrivendo le parole pronunciate, nel 2005, ai neolaureati di Stanford dall'uomo che più di ogni altro ha sfidato e vinto il futuro e la tecnologia: Steve Jobs.
"Il vostro tempo è limitato, per cui non lo sprecate vivendo la vita di qualcun altro. Non fatevi intrappolare dai dogmi, che vuol dire vivere seguendo i risultati del pensiero di altre persone. Non lasciate che il rumore delle opinioni altrui offuschi la vostra voce interiore. E, cosa più importante di tutte, abbiate il coraggio di seguire il vostro cuore e la vostra intuizione. In qualche modo loro sanno che cosa volete realmente diventare. Tutto il resto è secondario."

"Stay Hungry. Stay Foolish."
(Siate Affamati. Siate Folli.)
Steve Jobs
(1955-2011)

Ciò che auspicavo nelle considerazioni sopra trascritte nel novembre del 2011 a distanza di due anni è diventato realtà: il legislatore ha previsto, e non mi stancherò mai di ripeterlo, dal 30 giugno 2014 l'esclusività del deposito telematico di atti e documenti.
Il legislatore, forse anche e soprattutto spinto dalla necessità di razionalizzare ed abbattere i costi del servizio giustizia in un momento così delicato per il nostro Paese sotto il profilo economico, ha finalmente deciso di adottare, ed elevare a regola, l'utilizzo della tecnologia nell'esercizio della professione forense.
Adesso la sfida è ancora più bella e avvincente e potremo vincerla soltanto se i protagonisti del processo (avvocati, magistrati, dipendenti delle cancellerie), adesso si telematico, sapranno ben interpretare il ruolo affidato.
Perdere questa sfida significherebbe aver perso una grande occasione: innovare una professione rendendola più fluida, agevole e con risparmio di tempo e di costi per tutti i protagonisti coinvolti.
Come diceva Steve Jobs … *"Tutto il resto è secondario"*.