INFORMATICA GIURIDICA

collana diretta da Michele Iaselli

Numero 19

Il processo telematico

di Maurizio Reale

eBook
ALTALEX 2012

Le Collane

CIRCOLA
diretta da Raffaele Plenteda
Danni da animali randagi

CRIMINA
diretta da Simone Marani
Guida in stato di ebbrezza
Detenzione di stupefacenti: spaccio e uso personale
Il reato di stalking
I rimedi revocatori del giudicato penale
Il reato di violenza sessuale
Il reato di immigrazione clandestina
Stupefacenti: l'attenuante della lieve entità
Il processo penale minorile
Il reato circostanziato
La legittima difesa
Il delitto di furto
Pedopornografia
Il delitto di usura
I reati edilizi
Il delitto di rapina
I reati fallimentari
Il delitto di omicidio
Le frodi alimentari
La truffa
Il reato di sottrazione fraudolenta di imposte
Autovelox
La responsabilità penale del datore di lavoro
I reati tributari

DIRITTO DELLO SPORT
diretta da Gabriele Nicolella
Lavoro sportivo professionistico
Ordinamento e giustizia dello sport
Diritto penale sportivo
La previdenza sportiva
Giustizia sportiva nazionale e internazionale
Trasferimenti internazionali e normativa Fifa
Lavoro sportivo professionistico: l'imposizione sul reddito

FORMAZIONE
diretta da Luigi Viola
La contabilità degli studi professionali
L'affido condiviso
Provvedimenti cautelari d'urgenza
La testimonianza scritta
Le opposizioni nella procedura esecutiva
Mediazione e conciliazione
Pubblico spettacolo: disciplina delle opere

AMBIENTE E BENI CULTURALI
diretta da Alessandro Ferretti
La nuova autorizzazione paesaggistica
Il patrimonio culturale
La prelazione artistica
Energie rinnovabili: l'autorizzazione unica
I reati ambientali

INFORMATICA GIURIDICA
diretta da Michele Iaselli
Il Commercio Elettronico
Misure minime di sicurezza
La ricerca dei documenti giuridici
Privacy e marketing diretto
I nuovi reati informatici
Diritto d'autore e siti web
La PEC - Posta Elettronica Certificata
La prova digitale nel processo penale
Privacy e nuove tecnologie
Diritto e web 2.0
Consapevolezza fa rima con riservatezza
Cloud computing
Cyber stalking
Il processo telematico

MASSIMARIO
diretta da Luigi Viola
I maltrattamenti in famiglia
Decreto ingiuntivo
Violazione degli obblighi di assistenza familiare
Condominio

CODICI ALTALEX
Codice delle assicurazioni private
Codice della strada
Codice civile
Codice commentato del processo amministrativo
Codice del consumo
Codice della proprietà industriale
Codice di procedura civile
Testo unico degli Enti locali
Legge fallimentare
Testo unico per la sicurezza sul lavoro
Testo unico delle spese di giustizia
Codice penale
Codice di procedura penale
Testo unico commentato dell'immigrazione
Codice dell'ambiente
Legge di stabilità 2012
Codice degli appalti
Codice dell'amministrazione digitale commentato
Tabella dei costi chilometrici
Codice della mediazione e della conciliazione

FISCALE
diretta da Marco Palamidessi
L'esterovestizione societaria
Nuovo regime dei contribuenti minimi
Gli interessi anatocistici

LAVORO
diretta da Giuseppe De Marzo
Il contratto a progetto
Le prestazioni assistenziali

FAMIGLIA
diretta da Giuseppe De Marzo
Figli naturali e famiglia di fatto

IL PROCESSO 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 create in tempi passati e non più aggiornate.

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 quelle relative alle altre discipline. Tale "pigrizia" appare ancora più grave se si consideri che il corrente anno ha visto, sul piano normativo, il verificarsi di una vera e propria rivoluzione come tale potendosi definire il passaggio dalla CPECPT alla PEC come mezzo di comunicazione tra il professionista e il Gestore Centrale sia per il deposito telematico degli atti sia per le comunicazioni telematiche.

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.

Capitolo I
Le origini del PCT

Sommario: Premessa - 1.1. Le statistiche del PCT al 30 giugno 2011 - 1.1.1 Le statistiche del PCT al 30 giugno 2011: il deposito di atti e documenti telematici a valore legale - 1.1.2 Le statistiche del PCT al 30 giugno 2011: 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 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 benificiare 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 PCT al 30 giugno 2011

Le statistiche ufficiali del Ministero della Giustizia così come pubblicate sul sito dedicato al processo civile telematico[4] sono indicative di come nell'anno 2010 e nel primo semestre del 2011 si siano registrati indiscutibili progressi nell'avanzamento del programma di informatizzazione della giustizia civile italiana culminati con l'adozione di nuovi sistemi informativi dei registri di cancelleria: SIECIC e SICID.
Il sistema SIECIC per le esecuzioni civili individuali e concorsuali è attivo in tutti i 26 Distretti e, conseguentemente, funzionante in 165 su 165 Tribunali italiani.
Il sistema SICID per la cognizione civile (comprensivo del lavoro e della volontaria giurisdizione) è attivo in 18 Distretti su 26 per complessivi 127 Tribunali su 165.

[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://www.processotelematico.giustizia.it/.

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 23 Corti d'Appello e in 151 Tribunali e relative sezioni distaccate; per il processo esecutivo il servizio è attivo in 81 Tribunali.
Inoltre è stato istituito su tutto il territorio nazionale il sistema per la consultazione online dei procedimenti trattati dagli uffici dei Giudici di Pace.
In numerosi uffici è stato poi messo a disposizione un servizio di consultazione che consente agli avvocati di consultare online il fascicolo digitale che raccoglie gli atti ed i documenti del processo; tale servizio risulta attivo, per il processo di cognizione, in 10 Corti di Appello e in 89 Tribunali, mentre, per il processo di esecuzione, in 78 Tribunali. 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.

1.1.1 Le statistiche del P.C.T. al 30 giugno 2011: 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 30 giugno 2011, è attualmente attivo a valore legale in 33 Tribunali e relative sezioni distaccate e riguarda sia i procedimenti di ingiunzione, sia i procedimenti di esecuzione immobiliare, nonché il deposito delle memorie *ex* art. 183 c.p.c. e alcuni atti dei giudici.
Gli atti giudiziari depositati telematicamente nel solo 2010 ammontano a 50.785 unità mentre al 30 giugno 2011 ammontano a 42.238 unità[5].

1.1.2. Le statistiche del P.C.T. al 30 giugno 2011: 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 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.

[5] http://www.processotelematico.giustizia.it/pdapublic/resources/Statistiche_depositi_30giugno2011.pdf.

Tale funzione è stata attivata alla Corte di Appello di Milano, ai Tribunali di Bologna, Milano, Modena, Monza, Rimini nei cui circondari, con decreto ministeriale, è stata attribuita obbligatorietà e valore legale, con la conseguenza che le comunicazioni di cancelleria vengono effettuate esclusivamente per via telematica con significativa riduzione delle attività della cancelleria.
Il servizio è in corso di avvio alla Corte di Appello di Brescia, ai Tribunali di Brescia e di Torino (già emessi i decreti ministeriali), di Firenze, di Cremona e in tutti gli uffici giudiziari del distretto di Venezia (Corte di Appello inclusa).
Nel corso del 2010 sono state effettuate oltre 490.000 comunicazioni telematiche a valore legale ad oltre 12.000 avvocati la cui adesione ai servizi telematici giudiziari è cresciuta in maniera esponenziale, registrando incrementi dell'ordine del 70% su base annua. Si noti, a questo proposito, che gli «avvocati telematici» in Italia sono oltre 24.000[6].

[6]http://www.processotelematico.giustizia.it/pdapublic/resources/Statistiche_Comunicazioni_30giugno2011.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 tutti gli atti di parte;
- ricevere tutte le comunicazioni da parte dell'Ufficio Giudiziario;
- richiedere il rilascio di copie di atti;
- richiedere agli Uffici del Ruolo della Procura della Repubblica le informazioni ostensibili ex art. 335 c.p.p.;
- pagare le spese di giustizia (contributo unificato e diritti di copia).

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 (soprat-tutto 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 è necessario porre in essere una serie di passaggi obbligatori.
Nella prima fase, che possiamo definire preliminare a 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 affinchè 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, affinchè 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 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, anche se, nelle prossime pagine, vedremo come l'avvocato non telematico vada incontro ad alcune difficoltà.

Capitolo IV
Le nuove regole tecniche del processo telematico

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 febbario 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) affinchè 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 trasmissivone 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 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

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

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:

- consente l'accesso da parte dell'utente privato alle informazioni e ai provvedimenti giudiziari (art. 6, n. 1, D.M. 21 febbraio 2011, n. 44);
- mette 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);
- mette a disposizione i servizi di pagamento telematico (art. 6, n. 4, D.M. 21 febbraio 2011, n. 44);
- mette 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);
- consente l'accesso senza l'impiego di apposite credenziali, sistemi di identificazione e requisiti di legittimazione, alle informazioni ed alla docu-mentazione sui servizi telematici del dominio giustizia, alle raccolte giurisprudenziali e alle informazioni essenziali sullo stato dei proce-dimenti 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, complicherà ulteriormente le cose per gli addetti ai lavori in quanto soprattutto (ma non solo) la gestione delle ricevute potrebbe 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.
Al momento quindi è possibile affermare che tale Portale sembrerebbe esplicare solo ed esclusivamente la FUNZIONE DI CONSULTAZIONE di atti e/o documenti ma non anche quella preparatoria, propedeutica e successiva al deposito degli stessi.
La logica conseguenza è che i P.D.A. esterni svolgeranno (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 comuni-cazione 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).

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 per gli Ordini degli Avvocati sono previsti adempimenti la cui osservanza sarà determinante affinchè l'avvocato possa continuare la consultazione del Polisweb e operare con il processo telematico.
A tal proposito il Ministero della Giustizia ha diramato 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".***
Nello specifico l'Ordine dovrà:
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 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 all'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'elen-co 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@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 inesi-stente), sia ad errori legati a vincoli e prerequisiti

che presuppongono la validità dell'invio di un albo (ad esempio: censimento dell'ente richie-dente 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 informatiz-zazione 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 progres-sivamente 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 ammini-strazioni - e quindi condivide tra di essi - i propri sistemi attraverso l'erogazione via web di appli-cazioni 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 determi-nabili 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 sistematiz-zazione 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 pos-sesso 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 trattatamento. 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 garanzi 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, concre-tamente, 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
Processo telematico e proble-matiche giuridiche

Sommario: Premessa - 6.1. A rischio la certezza del deposito dell'atto o del documento informatico entro i termini stabiliti nel processo - 6.2. L'immediata visibilità dell'atto o della memoria depositata telematicamente è conforme a quanto dettato dal codice di procedura civile – 6.3. La presenza attuale e futura del documento cartaceo nel processo telematico e le connesse difficoltà dell'avvocato non telematico – 6.4. Le notifiche telematiche tra avvocati e l'art. 18, D.M. 21 febbraio 2011 n. 44 - 6.4.1 Le notifiche telematiche tra avvocati fino al 31 dicembre 2011 - 6.4.2. Le notifiche telematiche tra avvocati dal 01 gennaio 2012 - 6.5. - Il momento del perfezionamento della notifica

Premessa
Abbiamo visto nelle pagine precedenti come il passaggio alle nuove regole tecniche del processo telematico sia coinciso anche con quello, a carico del professionista, di alcuni rischi legati all'uso del mezzo informatico.
In questo capitolo affronteremo invece alcune problematiche di carattere giuridico relative all'utilizzo del processo telematico.

6.1. A rischio la certezza del deposito dell'atto o del documento informatico entro i termini stabiliti nel processo
Si trascrive, per comodità del lettore, l'art. 13 delle Regole Tecniche D.M. 21 febbraio 2011 n. 44:

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. Ai fini della comunicazione prevista dall'articolo 170, quarto comma, del codice di procedura civile, la parte che procede al deposito invia ai procuratori delle parti costituite copia informatica dell'atto e dei documenti allegati con le modalità previste dall'articolo 18 del presente decreto. Fuori del caso di rifiuto per omessa sottoscrizione, il rigetto del deposito da parte dell'ufficio non impedisce il successivo deposito entro i termini assegnati o previsti dal codice di procedura civile.
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 nonchè 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.
Tale articolo prevede, quindi, che

1. gli atti processuali in forma di documenti informatici sono trasmessi da parte dei soggetti abilitati esterni mediante PEC all'indirizzo PEC dell'Ufficio destinatario (art. 13 n.1 Regole Tecniche D.M. 21 febbraio 2011 n. 44).
2. Gli atti processuali in forma di documenti informatici si intendono ricevuti dal dominio giustizia nel momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di PEC del Ministero della Giustizia e ciò ai sensi e per gli effetti dell'art. 13 n. 2 Regole Tecniche D.M. 21 febbraio 2011 n. 44.
3. Se la ricevuta viene rilasciata dopo le ore 14.00, il citato articolo prevede che il deposito si considera effettuato il giorno feriale immediatamente successivo.

Tale norma mette a rischio la certezza del deposito dell'atto o del documento entro i termini stabiliti nel processo e ciò indipendentemente dalla volontà o dalla diligenza del professionista in quanto.
Supponiamo, per ipotesi, che la mia memoria ex art. 183 c.p.c. abbia come data di scadenza quella del 21 luglio 2011 e che in pari data, avvalendomi del PCT mediante la mia PEC invii il detto atto (atto processuale - documento informatico) all'ufficio giudiziario competente alle ore 09.00.
Immediatamente la mia PEC dovrebbe (e sottolineo dovrebbe) ricevere due attestazioni:
1) la **ricevuta di accettazione** a conferma della presa in carico del messaggio da parte del mio gestore di PEC (gestore del professionista).
2) la **ricevuta di avvenuta consegna** a conferma che il messaggio è stato effettivamente consegnato al destinatario (inviata dal gestore del destinatario = Ministero della Giustizia).
Teoricamente e, aggiungo, logicamente, dovrebbe essere la ricevuta di accettazione rilasciata dal gestore della mia PEC a far decorrere il momento del deposito della comparsa in quanto, la stessa contiene tutti i riferimenti temporali; purtroppo così non è in quanto, per avere certezza dell'avvenuto deposito, dovrò attendere la seconda ricevuta, quella di avvenuta consegna da parte del gestore di PEC del Ministero della Giustizia.
Se la ricevuta di consegna del gestore di PEC del Ministero della Giustizia venisse rilasciata comunque dopo le ore 14.00 (ad es. per problemi tecnici che già in un recentissimo passato e più di una volta hanno paralizzato l'attività del PCT) la "logica" conseguenza sarebbe quella di avere depositato fuori termine la mia memoria in quanto:
"…Quando la ricevuta è rilasciata dopo le ore 14 il deposito si considera effettuato il giorno feriale immediatamente successivo". (cfr. art. 13 n. 3 delle Regole Tecniche D.M. 21 febbraio 2011 n. 44)
e questo nonostante che l'atto sia stato "spedito" telematicamente da me in tempo utile ma non recapitato per responsabilità a me non addebitabile.

E allora mi chiedo: qualora si dovesse verificare tale o simile ipotesi, sarà applicabile quanto previsto dalla L. 69/2009, di modifica al codice di procedura civile, che ha aggiunto un secondo comma all'articolo 153 c.p.c., mediante il quale la parte che dimostra di essere incorsa in decadenze per causa ad essa non imputabile può chiedere al giudice di essere rimessa in termini?
E, pur ammessa l'utilizzabilità di tale norma, se il PCT deve avere come primo obiettivo quello di facilitare l'iter processuale e agevolare l'attività dei protagonisti è, per tale considerazione, impensabile che poi si debba far ricorso al disposto di cui all'art. 153 c.p.c. per rimediare ad una anomalia prevedibile e, in quanto tale, evitabile sin dall'origine.
Si consideri poi, in caso di istanza ex art. 153 c.p.c., la difficoltà di provare il presupposto per ottenere la rimessione in termini in quanto al Giudice (fino a quando sul punto non vi sia giurisprudenza) non potrebbe essere sufficiente l'attestazione di accettazione rilasciata dalla mia PEC considerando che per il legislatore il presupposto della certezza dell'avvenuto deposito è la seconda ricevuta, quella di consegna, emessa dal gestore di PEC del Ministero; occorrerebbe quindi una attestazione di tale ultimo gestore che riconosca il problema tecnico nel rilascio (posticipato) della ricevuta di consegna (avvenuta nei termini).
Probabilmente, a seconda dei casi o delle problematiche, tutti avremo la necessità di diventare profondi conoscitori dell'informatica forense (computer forensics) ossia la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico al fine di essere valutato e considerato come prova in un processo giuridico.
Qualcuno potrebbe suggerire (per superare il verificarsi di tale problema) di depositare l'atto qualche giorno prima rispetto al termine di scadenza in maniera tale di avere il tempo per effettuare una seconda spedizione telematica in assenza di ricevuta di consegna del gestore di PEC del Ministero della Giustizia; tale suggerimento, a mio avviso, è in re ipsa del tutto contrastante con i presupposti e le finalità del processo telematico.
Per cui, nell'auspicare una modifica normativa che possa eliminare il rischio dell'incertezza del deposito dell'atto o del documento informatico entro i termini stabiliti nel processo non posso, a conclusione di questa riflessione, non pormi una domanda: l'informatizzazione del processo deve sempli-ficare il lavoro di chi opera o renderlo ancora più difficile e insidioso?

6.2. L'immediata visibilità dell'atto o della memoria depositata telematicamente è conforme a quanto dettato dal codice di procedura civile

Nel giugno 2011, presso il Tribunale di Teramo, è iniziata la fase di sperimentazione del processo telematico. La stessa si è conclusa con esito positivo se è vero che in data 27 ottobre 2011, il Ministero della Giustizia ha emesso il decreto che attesta il valore legale di ciò che era oggetto della sperimentazione. Sin dal luglio 2010, in verità, il locale Consiglio dell'Ordine era pronto per consentire ai propri iscritti di iniziare la sperimentazione avendo ottemperato a tutti gli obblighi normativi previsti ed essendosi dotato di idoneo partner tecnologico ma la struttura giudiziaria non era ancora pronta ad interagire con le nuove e innovative tecnologie.
A differenza delle altre precedenti sperimentazioni relative, nella fase primordiale, soprattutto al deposito dei decreti ingiuntivi telematici, a Teramo la stessa ha avuto ad oggetto il deposito di memorie ex art. 183 c.p.c., comparse di costituzione e risposta, comparse conclusionali, note, note spese e qualsiasi altro atto previsto dal processo di cognizione per il quale però non si dovesse corrispondere, per il deposito, alcun tipo di pagamento.
Proprio questo tipo di sperimentazione mi ha dato la possibilità di verificare la seguente situazione che andrò ad enunciare dopo una dovuta riflessione.

In venti anni di professione forense non ho mai ricevuto dalle cancellerie dei Tribunali che ho frequentato, la memoria o l'atto avversario se non dopo aver depositato il mio o dopo la scadenza del termine per il mio deposito. Onestamente non mi sono nemmeno mai sognato di chiedere all'impiegato della cancelleria, in assenza di mio deposito o di scadenza del termine, la consegna della memoria della mia controparte e, sinceramente, nemmeno mi sono mai chiesto se vi fosse una norma del codice di procedura civile che consentisse tale richiesta.
Fatta questa premessa, attraverso la sperimentazione del Tribunale di Teramo, ho rilevato che la memoria depositata telema-ticamente è immediatamente visibile (tramite Polisweb PCT) alla controparte anche se questa non ha depositato la propria e se non è ancora scaduto il termine per il suo deposito. Sinceramente la cosa mi ha un po' stupito in quanto ritenevo che ciò non fosse possibile considerando che la lettura anticipata della memoria di una parte potrebbe consentire all'altra di elaborare la propria in ragione di quanto dedotto nell'atto avversario; tale rischio è a mio avviso, ancora più evidente qualora il contenuto dell'atto conosciuto sia quello riferibile alla memoria di replica di una comparsa conclusionale o di qualsiasi altro atto che non preveda comunque successive repliche.
Ponevo quindi il quesito ai circa 2.400 colleghi iscritti di un gruppo che amministro su Facebook e potevo rilevare come, in realtà non solo non fossi l'unico a pensarla così ma che la molti di coloro che hanno risposto alla domanda aveva la mia stessa convinzione anche se… alla richiesta di citare la norma in base al quale ciò non era consentito, nessuno sapeva indicarla limitandosi, qualcuno, a dire che il divieto era insito nel fatto che si sarebbe leso il principio del contrad-dittorio.
Per dovere di verità devo aggiungere che la norma non veniva citata neanche da parte di coloro che sostenevano la legittimità del ritiro dell'atto in assenza del deposito del proprio o della scadenza del termine.
La norma esiste ed è quella prevista **dall'art. 76 delle Disposizioni di attuazione del codice di procedura civile:**

Art. 76. Potere delle parti sui fascicoli
Le parti o i loro difensori muniti di procura possono esaminare gli atti e i documenti inseriti nel fascicolo d'ufficio e in quelli delle altre parti e farsene rilasciare copia dal cancelliere, osservate le leggi sul bollo. ***(Comma così modificato dall'art. 7 d.l. 07 ottobre 1994, n. 571, conv., con modif., in l. 6 dicembre 1994 n. 673.)***
La norma citata quindi consente il ritiro dell'atto o della memoria depositata da controparte anche se l'altra parte non abbia ancora depositato e non sia scaduto il termine per il deposito.
Per cui non rimane altro che depositare l'atto in prossimità della scadenza del termine anche se, con il deposito telematico questo può compor-tare fondati rischi per quanto dettato dall'Art. 13 delle regole tecniche del D.M. 21 febbraio 2011 n. 44 e di cui ho ampiamente criticato il contenuto nelle pagine precedenti.
Quanto da me dedotto nel presente paragrafo ha trovato puntuale conferma nella comunicazione del Tribunale di Teramo datata 17 novembre 2011 ed inoltrata agli avvocati del Foro di Teramo dal locale Consiglio dell'Ordine il 17 novembre 2011 e di cui potrete prenderne visione qui.

6.3. La presenza attuale e futura del documento cartaceo nel processo telematico e le connesse difficoltà dell'avvocato non telematico
L'esame del D.M. 21.02.2011 n. 44 e delle specifiche tecniche del 18 luglio 2011 mi aveva consentito di dimostrare come fosse a rischio la certezza del deposito dell'atto e/o del documento informatico entro i termini processuali;

qui evidenzierò, nelle medesime norme, la presenza di alcune incongruenze, che stridono con le più elementari finalità del processo telematico di seguito riepilogate:

3) passaggio dal cartaceo al digitale
4) risparmio carta
5) recupero di spazi
6) vantaggi per il professionista
7) vantaggi per le cancellerie

Prendiamo in esame un caso concreto e quindi un Tribunale al quale il Ministero della Giustizia abbia rilasciato il decreto attestante il valore legale dei depositi telematici relativi a memorie, comparse, documenti ecc. ecc.
In tale situazione, pur in presenza del valore legale, gli avvocati saranno sempre liberi di scegliere se depositare la propria memoria nella maniera tradizionale (recandosi in Cancelleria) o attraverso il mezzo telematico; questo perché al momento non esiste una norma per la quale l'avvocato, concesso il valore legale ad un Tribunale, sia obbligato al deposito dell'atto in via telematica così come simile norma invece esiste, nel momento in cui il valore legale venga riconosciuto per l'invio delle comunicazioni telematiche (biglietti di cancelleria) le quali, decorsi gg. 15 dalla pubblicazione in Gazzetta Ufficiale del decreto, verranno effettuate solo ed esclusivamente tramite PEC giusto il disposto dell'art. 4 L. 24/2010.
Nel caso preso in esame potrà verificarsi tra l'Avvocato Tizio e l'Avvocato Caio questa situazione:
l'Avvocato Tizio deposita la sua memoria istruttoria con 30 allegati servendosi del mezzo telematico.
l'Avvocato Caio depositerà direttamente in Cancelleria la sua memoria istruttoria con 25 allegati. non disponendo della firma digitale e non essendo iscritto al P.D.A. o al Portale dei Servizi Telematici del Ministero della Giustizia e non avendo quindi neanche l'accesso al POLISWEB PCT.
In questa situazione si applica, per il deposito dell'Avv. Caio, quanto previsto dalle nuove regole tecniche e più precisamente l'art. 14 del D.M. 21.02.2011 n. 44 e l'art. 15 delle specifiche tecniche del 18 luglio 2011 che prevedono la possibilità di depositare documenti probatori e allegati in formato non elettronico **ponendo a carico della Cancelleria l'elaborazione di una copia informatica degli stessi e il successivo inserimento nel fascicolo informatico.**
Da ciò ne deriva che:

8) la Cancelleria dovrà tempestivamente elaborare (scansionare) la memoria e i 25 allegati dell'Avvocato Caio avendo cura di depositare il tutto nel fascicolo informatico e,
9) l'Avvocato Tizio, telematico, avrà la possibilità, tramite POLISWEB PCT di visionare e stampare (tramite computer del proprio Studio) quanto depositato su carta dal collega Caio a seguito della elaborazione informatica eseguita dalla Cancelleria.

Già da questa considerazione è facile rilevare come la Cancelleria, nonostante il deposito telematico dell'Avvocato Tizio e il tempo guadagnato per il fatto che il detto Avvocato non si sia presentato in Cancelleria, abbia comunque impiegato del tempo per scansionare gli atti dell'Avvocato Tizio (probabilmente un tempo maggiore di quello guadagnato per il mancato accesso dell'Avvocato telematico).
Viene in questa maniera meno, quindi, uno dei vantaggi del processo telematico ossia il risparmio di tempo da parte della Cancelleria.
Ma questo non è l'unico (grave) disagio.
Passiamo ad esaminare la posizione dell'Avvocato non telematico; l'Avvocato Caio ha infatti la necessità di avere copia della memoria e dei documenti depositati telematicamente dall'Avv. Tizio ma, come detto, non essendo avvocato telematico non possiede neanche il POLISWEB (e finora

nessuno può obbligarlo ad averlo!) per cui non potrà accedere al fascicolo informatico del procedimento che lo riguarda.
Le regole tecniche del PCT (D.M. 22.02.2011 n. 44 e specifiche tecniche del 18 luglio 2011) nulla dicono per tale situazione per cui la Cancelleria, a mio avviso, non sarebbe obbligata e quindi tenuta a stampare la documentazione depositata telematicamente al fine di consegnarla all'Avv. Caio.
A questo punto vediamo, quindi, quale tra le norme esistenti dovrà e potrà applicarsi al caso di specie al fine di consentire all'Avvocato Caio di conoscere e di acquisire quanto depositato telematicamente dall'Avv. Tizio.
La prima norma che potrebbe applicarsi è quella di cui all'art. 170, 4° comma c.p.c.:

Art. 170. - Notificazioni e comunicazioni nel corso del procedimento
Dopo la costituzione in giudizio [c.p.c. 165, 166] tutte le notificazioni e le comunicazioni si fanno al procuratore costituito, salvo che la legge disponga altrimenti [c.p.c. 237, 286, 292, 306, 330] (1).
E' sufficiente la consegna di una sola copia dell'atto anche se il procuratore è costituito per più parti.
Le notificazioni e le comunicazioni alla parte che si è costituita personalmente si fanno nella residenza dichiarata o nel domicilio eletto [c.p.c. 30, 82].
Le comparse [c.p.c. 190] e le memorie consentite dal giudice si comunicano mediante deposito in cancelleria oppure mediante notificazione o mediante scambio documentato con l'apposizione sull'originale, in calce o in margine, del visto della parte o del procuratore. Il giudice può autorizzare per singoli atti, in qualunque stato e grado del giudizio, che lo scambio o la comunicazione di cui al presente comma possano avvenire anche a mezzo telefax o posta elettronica nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici e teletrasmessi. La parte che vi procede in relazione ad un atto di impugnazione deve darne comunicazione alla cancelleria del giudice che ha emesso la sentenza impugnata. A tal fine il difensore indica nel primo scritto difensivo utile il numero di telefax o l'indirizzo di posta elettronica presso cui dichiara di voler ricevere le comunicazioni (2).
Ma, tale norma, non fa al caso nostro in quanto se è vero come è vero che il decreto che attesta il valore legale in un Tribunale equipara il deposito telematico e quello cartaceo in Cancelleria si comprende benissimo come, chi deposita telematicamente, abbia dato seguito a quanto richiesto dalla norma in oggetto ed evidenziata in neretto e non abbia quindi bisogno di replicare il deposito del cartaceo anche in Cancelleria.
L'art. 170 Codice di Procedura Civile quindi non potrà essere d'aiuto all'Avv. Caio.
A questo punto non rimane altro da fare se non confrontarsi con l'art. 76 delle disposizioni di attuazione al c.p.c.

Art. 76. - Potere delle parti sui fascicoli
Le parti o i loro difensori muniti di procura possono esaminare gli atti e i documenti inseriti nel fascicolo d'ufficio e in quelli delle altre parti e farsene rilasciare copia dal cancelliere, osservate le leggi sul bollo.
In base a tale disposto normativo l'Avv. Caio può risolvere il suo problema ma dovrà:

10) accontentarsi di esaminare (dove? tramite monitor del PC dell'impiegato di cancelleria?) i documenti depositati telematicamente dall'Avvo-cato Tizio o

11) farsi rilasciare, dal Cancelliere, copia degli atti e dei documenti OSSERVATE LE LEGGI SUL BOLLO = PAGARE I DIRITTI RELATIVI ALLE COPIE RICHIESTE E RILASCIATE = PAGARE PER AVERE COPIA DI QUANTO DEPOSITATO DA CONTROPARTE TELEMATICAMENTE.

L'Avv. Caio quindi per risolvere il suo problema (acquisizione di quanto depositato dall'Avvocato telematico, o dovrà munirsi quanto meno di firma digitale e di accesso al POLISWEB PCT o dovrà pagare i diritti di cancelleria per il rilascio degli atti depositati telematicamente da controparte in quanto…

…riepilogando:

nessuna norma o regole tecnica permette al Cancelliere di stampare e consegnare, sic et simpliciter, alla parte costituita a mezzo di avvocato non telematico, la memoria e la documentazione depositata dall'Avvocato Tizio se non a seguito del pagamento dei diritti di copia a meno di non rischiare di incorrere, in caso di ispezioni, in personali responsabilità derivanti dalla mancata percezione degli importi inerenti le copie rilasciate.

Per analogia è conforme alla soluzione proposta quanto dedotto e comunicato dal Presidente del Tribunale per i Minorenni di Venezia, Dott. Adalgisa Fraccon, con la nota del 28/03/2011 prot. n. 52[11] (di seguito trascritta unitamente alle note del Ministero citate) risolutiva della problematica sorta circa il pagamento o meno dei diritti di copia mediante l'utilizzo, da parte degli avvocati, di scanner portatili idonei ad acquisire copia degli atti processuali.

«È stato rilevato che alcuni difensori estraggono copia degli atti processuali mediante l'uso di scanner portatili ovvero che estraggono copia di atti e documenti contenuti in CD o DVD, mediante trasferimento degli stessi su supporti portatili come ad esempio chiavette USB.

«Queste nuove modalità di estrazione delle copie pongono dei problemi per quanto riguarda il pagamento dei diritti di copia, visto che tali procedure non sono espressamente previste dalla normativa vigente. Tuttavia si ritiene che proprio in base alle disposizioni emanate dal legislatore e dal Ministero il problema possa essere risolto nel modo che segue.

«Per quanto riguarda le copie scannerizzate, le cancellerie avranno cura di far pagare i relativi diritti di copia secondo i normali canoni previsti per le copie cartacee secondo le tabelle già note. A questo proposito si ribadisce che l'esazione del diritto di copia deriva da una disposizione di natura fiscale e non costituisce una forma di rimborso per l'uso di fotocopiatrice, carta ed inchiostro (vedi le due note allegate del Ministero).

«Diverso è il problema per ciò che concerne l'uso di dispositivi portatili come chiavette USB o addirittura PC, per la copia di materiale contenuto in CD e DVD. Ebbene **per motivi di sicurezza informatica è assolutamente vietato collegare dispositivi del genere ai computer dell'Amministrazione.** È evidente infatti da un lato che nel dispositivo utilizzato dall'utenza potrebbero essere contenuti, sia pure inconsapevolmente, virus o altri files che potrebbero non solo il singolo PC cui si collega, ma in astratto tutte le macchine collegate alla Rete Giustizia. Inoltre mentre un file copiato su DVD non riscrivibile, non è modificabile e non può dar luogo a nessuna contestazione, un file copiato su dispositivi come quelli in parola può essere facilmente modificato e quindi potenzialmente dar luogo a contestazioni. In conclusione qualora una parte abbia interesse a copiare atti e documenti contenuti su CD o DVD, dovrà chiederne copia su supporto analogo e pagare i diritti di cancelleria previsti dalla vigente normativa.»

Di seguito, si riportano le note del Ministero della Giustizia, Dipartimento per gli Affari di Giustizia, Direzione Generale della Giustizia Civile citate nel testo della Presidente.

[11] Pubblicata sul sito www.trivenews.it e consultabile qui.

Nota del 13 settembre 2006: «(OMISSIS) **se siano dovuti i diritti di copia nel caso in cui le parti processuali provvedano direttamente alle spese per il rilascio di copia**. Trattasi nel caso specifico di dover provvedere al rilascio di centinaia di migliaia di copie relative a documentazione sequestrata ed affidata in custodia per le quali l'ufficio sopra menzionato asserisce di non poter provvedere, per carenza di fondi e strutture organizzative (macchinari, carta, personale, ecc.). e che, pertanto, le medesime dovranno essere necessariamente effettuate, a spese delle parti, da una copisteria sono la diretta responsabilità del custode.
«Con riferimento alla sopra esposta problematica la scrivente Direzione Generale è del parere che l'esazione dei diritti di copia deve avvenire nella misura fissata dal legislatore secondo la tariffa prevista dalla relativa tabella allegata al D.P.R. 115/2002.
«Trattasi. infatti, di una disposizione di natura fiscale non altrimenti derogabile anche nei casi, del tutto eccezionali, ove per esigenze processuali il rilascio di rilevanti quantità di copie non può essere fronteggiato con l'ausilio del personale in servizio (anche ricorrendo ad eventuali applicazioni temporanee) e dei mezzi tecnici in possesso dell'ufficio.»

Nota del 27 febbraio 2007: «(*Omissis*) **se sia dovuta la maggiorazione del diritto di copia quando il richiedente non manifesti l'urgenza e, comunque, le medesime vengano rilasciate entro due giorni dalla richiesta**.
Con riferimento all'accennata problematica la scrivente Direzione Generale è del parere che l'esazione del diritto di copia deve avvenire nella misura fissata dal D.P.R. 115/2002.
«In particolare l'art. 270 della richiamata disposizione legislativa prevede la triplicazione del diritto di copia quando il rilascio, su supporto cartaceo senza e con certificazione di conformità, avviene entro due giorni dalla richiesta.
«Trattasi di una disposizione di natura fiscale, non altrimenti derogabile, in cui i termini dell'urgenza sono fissati dal legislatore, e non dalla parte richiedente.
«Ne discende, quindi, che, nell'ipotesi di rilascio di copie nel temine dei due giorni, è dovuta la maggiorazione che si aggiunge al diritto fissato in via ordinaria.»

6.4. Le notifiche telematiche tra avvocati e l'art. 18 del D.M. 21 febbraio 2011, n. 44

Premessa

Devo confessare al lettore che il contenuto di tale articolo è stato interamente rivisitato a seguito delle novità legislative approvate il 12 novembre 2011 ed inserite nella Legge di Stabilità la cui entrata in vigore (per la maggior parte di esse) è prevista per il 01 gennaio 2012.
Alcune di queste modifiche sono state dedicate dal legislatore all'utilizzo della posta elettronica certificata nel processo civile e, aggiungo in anticipo, hanno eliminato una grossa illogicità che però rimarrà fino all'entrata in vigore della nuova normativa.
Ritenendo comunque, importante enunciare cosa sarebbe continuato ad accadere in assenza di tali modifiche legislative, descriverò sia l'attuale disciplina delle notifiche telematiche tra avvocati sia quella in vigore dal 01 gennaio 2012.

6.4.1 Le notifiche telematiche tra avvocati fino al 31 dicembre 2011

L'art. 18 delle regole tecniche del D.M. 21 febbraio 2011, n. 44 prevede che nel caso previsto dall'articolo 4, legge 21 gennaio 1994, n. 53 *"…il difensore può eseguire la notificazione ai soggetti abilitati esterni con mezzi telematici, anche previa estrazione di copia informatica del documento cartaceo".*
A tale scopo l'avvocato:

1) trasmette copia informatica dell'atto sottoscritta con firma digitale all'indirizzo di posta elettronica certificata del destinatario risultante dal registro generale degli indirizzi elettronici, nella forma di allegato al messaggio di posta elettronica certificata inviato al destinatario.
2) inserisce la relazione di notificazione che contiene le informazioni di cui all'articolo 3, comma 2, della legge 21 gennaio 1994, n. 53, dell'indirizzo di posta elettronica certificata presso il quale l'atto è stato inviato, nonché del numero di registro cronologico di cui all'articolo 8 della suddetta legge.

La notificazione si intende perfezionata nel momento in cui viene generata la ricevuta di avvenuta consegna breve da parte del gestore di posta elettronica certificata del destinatario.
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.
Bene, facendo riferimento le regole tecniche al caso previsto dall'articolo 4 della legge 21 gennaio 1994 n. 53 è opportuno trascrivere il testo di tale articolo affinchè possa comprendersi come la stessa non sia aderente alla logica del processo telematico motivo per cui sarebbe stato meglio modificarla in relazione a quanto dalla medesima previsto al n. 2:

Legge 21.01.1994 n. 53

Articolo 4 - 1. L'avvocato o il procuratore legale, munito della procura e dell'autorizzazione di cui all'articolo 1[12], 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 e che sia iscritto nello stesso albo del notificante.
2. Nel caso di cui al comma 1**, l'originale e la copia dell'atto devono essere previamente vidimati e datati dal consiglio dell'ordine nel cui albo entrambi sono iscritti**.
La norma quindi, non modificata e applicabile conseguentemente anche all'ipotesi prevista dall'art. 18 del D.M. 21.02.2011 n. 44, impone all'avvocato di recarsi presso l'Ordine in cui entrambi i professionisti sono iscritti, con l'atto cartaceo (!) sul quale far apporre la vidimazione e la data.
Simuliamo lo schema di una notifica telematica ai sensi del combinato disposto dell'art. 4 della L. 21.01.1994 n. 53 e dell'art. 18 D.M. 21.02.2011 n. 44:
1) il professionista redige il proprio atto (informatico) da notificare;
2) deve necessariamente estrapolare dall'atto informatico quello cartaceo (stampa dell'atto informatico);
3) deve recarsi presso gli uffici dell'Ordine con il proprio atto cartaceo affinchè l'Ordine possa vidimarlo e datarlo;
4) deve tornare in studio e qui estrapolare dall'atto cartaceo quello informatico (mediante scanner);
5) deve firmare digitalmente l'atto informatico da notificare a mezzo pec;
6) eseguita questa procedura finalmente potrà inviare al collega, a mezzo pec e sotto forma di allegato, l'atto oggetto di notifica.

[12] 1.L'avvocato o il procuratore legale, munito di procura alle liti a norma dell'art. 83 del codice di procedura civile e della autorizzazione del consiglio dell'ordine nel cui albo è iscritto a norma dell'art. 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, salvo che l'autorità giudiziaria disponga che la notifica sia eseguita personalmente.

Ma … è logico che per la notifica telematica tra avvocati non si possa prescindere dal documento cartaceo?
E' altresì logico che, nonostante la sottoscrizione del documento con firma digitale (che attesta l'identità del professionista e il momento temporale della "firma") non si possa prescindere dal far apporre dall'Ordine la vidimazione e la data sul cartaceo?
Una portata logica tale procedura cartacea-telematica, non la ha a meno che… il fine non sia quello di scoraggiare il professionista all'utilizzo dell'art. 18, D.M. 21 febbraio 2011 n. 44.

6.4.2 Le notifiche telematiche tra avvocati dal 1 gennaio 2012

Con la legge sulla Stabilità sono state apportate, come detto, modifiche sia al codice di procedura civile sia alla Legge 21 gennaio 1994, n. 53 ed è proprio grazie a tali modifiche che la situazione descritta nel paragrafo precedente è radicalmente cambiata (o meglio cambierà dal 01 gennaio 2012) essendo stato di fatto cancellato l'obbligo per l'avvocato previsto dal comma 2 dell'art. 4 L. 21.01.94 n. 53 di far vidimare e datare il proprio atto dal Consiglio dell'Ordine prima di notificare telematicamente lo stesso.
Ma vediamo la nuova formulazione del citato articolo:

Legge 21 gennaio 1994, n. 53
(a seguito delle modifiche introdotte dalla Legge sulla Stabilità del 12 novembre 2011)

Art. 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 a mezzo posta elettronica certificata, ovvero** 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.**
È stato quindi parzialmente integrato il comma 1 e interamente sostituito il comma 2 dell'art. 4, L. 21 gennaio 1994, n. 53 il quale adesso prevede l'obbligo per l'avvocato di far vidimare e datare l'atto da notificare solo e soltanto qualora decida di effettuare la notifica mediante consegna tradizionale e non anche mediante utilizzo della posta elettronica certificata.
Nel comma 1 è stata altresì eliminata la parte che limitava le notifiche telematiche ai soli avvocati appartenenti allo stesso Ordine essendo quindi ora ammessa anche la notifica tra avvocati appartenenti a Ordini diversi.
Altra modifica (di portata generale e non specifica alle notifiche tra avvocati) è quella prevista all'art. 3 della L. 21.01.94 n. 53 la quale, in riferimento all'art. 1 della stessa legge, da una parte consente all'avvocato di effettuare notifiche (a non avvocati) a mezzo della posta elettronica certificata ponendo come condizione da una parte che l'indirizzo del destinatario risulti da pubblici elenchi e che dall'altra si osservino le modalità previste, per gli Ufficiali Giudiziari, dall'art. 149 bis del codice di procedura civile in quanto compatibili.

6.5. - Il momento del perfezionamento della notifica

Risolta l'anomalia evidenziata nel precedente paragrafo ne sottopongo, all'attenzione del lettore, un'altra anch'essa inserita nell'articolo 18 così come rilevata dall'Avv. Giorgio Battaglini e dallo stesso illustrata nel corso di un convegno tenutosi a Venezia il 22 giugno 2011[13].
Evidenzia il collega come, ai sensi dell'art. 18 del D.M. 21 febbraio 2011, n. 44, la notificazione si intende perfezionata nel momento in cui viene generata la ricevuta di avvenuta consegna breve da parte del gestore di posta elettronica certificata del destinatario, chiedendosi, giustamente, se tale norma non sia in contrasto con la attuale formulazione dell'art.149 c.p.c. [14]il quale prevede che la notifica si perfezioni per il notificante al momento della consegna dell'atto all'ufficiale giudiziario[15] e, per il destinatario, dal momento in cui lo stesso ha la legale conoscenza dell'atto.
Per cui se notifichiamo:

1) tramite Ufficiale Giudiziario, l'atto si intende depositato nel momento in cui lo stesso viene consegnato all'Ufficio Unep;
2) telematicamente la stessa si intende perfezionata nel momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del destinatario.

Nella notifica telematica effettuata ai sensi dell'art. 18, D.M. 21 febbraio 2011 il perfezionamento della notifica coincide, sia per chi notifica sia per chi riceve la notifica, nel momento in cui viene generata la ricevuta di avvenuta consegna breve da parte del gestore di posta elettronica certificata del destinatario.
E' dimostrato quindi come venga disapplicato il disposto del secondo comma dell'art. 149 c.p.c. il quale invece prevede, per il perfezionamento della notifica, due diversi momenti: uno per chi notifica e l'altro per il destinatario della notifica.

[13] Intervento dell'Avv. Giorgio Battaglini al Convegno organizzato dall' Ordine degli Avvocati di Venezia e dalla Corte d'Appello di Venezia il 22 Giugno 2011 dal tema: *LE REGOLE TECNICHE PER L'ADOZIONE DELLE TECNOLOGIE DELL'INFOR-MAZIONE E DELLA COMUNICAZIONE NEL PROCESSO CIVILE E NEL PROCESSO PENALE*.
[14] Comma aggiunto dalla legge 263/2005, con decorrenza dal 1 marzo 2006.
[15] La Corte Costituzionale con sentenza 26 novembre 2002, n. 477 ha dichiarato l'illegittimità costituzionale del combinato disposto del presente articolo e dell'art. 4, comma terzo, della legge 20 novembre 1982, n. 890 (Notificazioni di atti a mezzo posta e di comunicazioni a mezzo posta connesse con la notificazione di atti giudiziari) nella parte in cui prevede che la notificazione si perfeziona, per il notificante, alla data di ricezione dell'atto da parte del destinatario anziché a quella, antecedente, di consegna dell'atto all'ufficiale giudiziario.

Capitolo VII
La vigilia del 19 novembre 2011

Il 21 ottobre 2011 inviavo per il mio Ordine, quale delegato alla firma e all'invio dell'albo, il documento di censimento e restavo in attesa di ricevere la risposta di D.G.S.I.A. a seguito della quale avrei poi potuto inviare l'albo degli iscritti in formato xml nel rispetto della nuova normativa.
Alla vigilia del 19 novembre 2011, giorno indicato da D.G.S.I.A. per il passaggio dalla CPECPT alla PEC per tutte le trasmissioni telematiche in ingresso e in uscita (depositi e comunicazioni) e per la definitiva applicazione delle regole tecniche indicate nel D.M. 21.02.2011 e delle specifiche tecniche del 18 luglio 2011, da D.G.S.I.A. all'indirizzo PEC del mio Ordine, nessuna risposta risultava pervenuta a seguito dell'invio del documento di censimento.
Teoricamente quindi, non avrei potuto compiere il passo successivo: l'invio dell'albo degli iscritti.
Ciò avrebbe comportato l'impossibilità per gli avvocati di Teramo di utilizzare il PCT.
Nella certezza di aver rispettato il protocollo stabilito da D.G.S.I.A. per l'invio del documento di censimento e nella ulteriore certezza quindi che fosse D.G.S.I.A. a non aver rispettato il disposto dell'art. 8 comma 3 del provvedimento 18 luglio 2011 ("specifiche tecniche") non avendo fatto pervenire risposta alcuna a seguito della ricezione del documento di censimento del mio Ordine, decidevo di inoltrare comunque all'indirizzo PEC comunicazionesoggetti@giustiziacert.it l'albo degli iscritti in formato xml.
Inviavo il file alle 17.35.
Non vi nascondo che controllavo la PEC a brevissimi intervallo di tempo.

Alle 20,41, nella mia PEC, giungeva il seguente messaggio che trascrivo integralmente:
Oggetto: [REGINDE] AVVENUTA REGISTRAZIONE AL PROCESSO TELEMATICO
Da: comunicazionesoggetti@giustiziacert.it
Data: Ven 18/11/2011 20:41
A: xxxxxxxxx.xxxxxx@pec-avvocatixxxxxxxx.it
Gentile Maurizio REALE
il suo indirizzo di PEC xxxxxxx.xxxxx@pec-avvocatixxxxxx.it è stato comunicato dal suo Ordine Professionale o Ente di appartenenza al Ministero della Giustizia e censito nel Registro Generale degli Indirizzi Elettronici ai sensi del D.M. 21 febbraio 2011 n. 44, art. 7.
Si prega di non replicare a questo messaggio automatico.
Per ulteriori informazioni:
http://www.processotelematico.giustizia.it/
Cordiali saluti.

Alle 20,56, nella PEC dell'Ordine, giungeva il seguente messaggio che trascrivo, anche questo, integralmente:

Oggetto: [REGINDE] OPERAZIONE ESEGUITA
Da: comunicazionesoggetti@giustiziacert.it
Data: Ven 18/11/2011 20:56
A: ordine@pec-avvocatixxxxxxxxx.it
Operazione completata con successo.
Controllare il file Esiti.xml in allegato per dettagli relativi.

Il primo messaggio comunicava la mia registrazione al processo telematico e l'inserimento del mio indirizzo PEC al Registro Generale degli Indirizzi Elettronici.
Analogo messaggio giungeva ad ogni iscritto dell'Ordine il cui nominativo era presente nell'Albo inviato.
Il secondo messaggio attestava che l'invio dell'Albo era andato a buon fine, pur in assenza della risposta da parte di D.G.S.I.A. prevista dell'art. 8 comma 3 del provvedimento 18 luglio 2011 ("specifiche tecniche") e, a tal proposito mi auguro che, pur in mancanza della detta risposta, i delegati degli Ordini abbiano comunque inviato l'albo degli iscritti in formato xml al fine di non compromettere l'accesso dei loro iscritti dal PCT.

Capitolo VIII
La normativa vigente del processo telematico

Sommario: 7.1. Il D.M. 21 febbraio 2011, n. 44 – 7.2 Le specifiche tecniche del 18 luglio 2011

7.1. Il D.M. 21 febbraio 2011, n. 44

Decreto del Ministro della giustizia in data 21 febbraio 2011 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.»

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 L. 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'ammini-strazione 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;

ADOTTA
IL SEGUENTE REGOLAMENTO:

CAPO I – PRINCIPI GENERALI

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 domi-nio 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 e successive modificazioni;
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 auto-matizzati 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 eli-minare lo spam;
t) **log**: documento informatico contenente la registrazione cronologica di una o più operazioni informatiche, generato automaticamente dal si-stema 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 è 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 di cui 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'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.

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 si-curezza 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 è 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 è 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, racco-gliendo 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. Ai fini della comunicazione prevista dall'articolo 170, quarto comma, del codice di procedura civile, la parte che procede al deposito invia ai procuratori delle parti costituite copia informatica dell'atto e dei documenti allegati con le modalità previste dall'articolo 18 del presente decreto. Fuori del caso di rifiuto per omessa sottoscrizione, il rigetto del deposito da parte dell'ufficio non impedisce il successivo deposito entro i termini assegnati o previsti dal codice di procedura civile.
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 nel fascicolo informatico, previa attestazione del deposito da parte della cancelleria o della segreteria dell'ufficio giudiziario mediante apposizione della data e della propria firma digitale.
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 vi appone la sua firma digitale, ove previsto.

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 breve 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, si procede ai sensi dell'articolo 51, comma 3 del decreto legge 25 giugno 2008 n. 112, convertito con modificazioni dalla legge 6 agosto 2008, n. 133, e successive modificazioni, nel caso in cui viene generato un avviso di mancata consegna previsto dalle regole tecniche della posta elettronica certificata.
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 breve 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 in-formatico 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 dal-la 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 nei modi di cui agli articoli 138 e seguenti del codice di procedura civile.

ART. 18

(Notificazioni per via telematica tra avvocati)

1. Nel caso previsto dall'articolo 4, legge 21 gennaio 1994, n. 53, il difensore può eseguire la notificazione ai soggetti abilitati esterni con mezzi telematici, anche previa estrazione di copia informatica del documento cartaceo. A tale scopo trasmette copia informatica dell'atto sottoscritta con firma digitale all'indirizzo di posta elettronica certificata del destinatario risultante dal registro generale degli indirizzi elettronici, nella forma di allegato al messaggio di posta

elettronica certificata inviato al destinatario. Nel corpo del messaggio è inserita la relazione di notificazione che contiene le informazioni di cui all'articolo 3, comma 2, della legge 21 gennaio 1994, n. 53, dell'indirizzo di posta elettronica certificata presso il quale l'atto è stato inviato, nonché del numero di registro cronologico di cui all'articolo 8 della suddetta legge. La notificazione si intende perfezionata nel momento in cui viene generata la ricevuta di avvenuta consegna breve da parte del gestore di posta elettronica certificata del destinatario.
2. Quando il difensore procede ai sensi dell'articolo 170, comma 4, del codice di procedura civile, la comunicazione delle memorie è effettuata mediante invio di copia della memoria alle parti costituite a mente 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.

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 regi-stri 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 prelimina-ri 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 pro-cedimenti 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 automa-tizzati.

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 requi-siti 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 d 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 auto-matizzati 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. È 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 autoriz-zato 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 garantisce 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 trentuno 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 river-samento 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 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, è 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 struttu-razione 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.
Dato a Roma, addì 21 febbraio 2011
Il Ministro della Giustizia
On. Avv. Angelino Alfano
Il Ministro per la Pubblica Amministrazione e l'Innovazione
On. Prof. Renato Brunetta
Visto, il Guardasigilli
On. Avv. Angelino Alfano
Registrato alla Corte dei Conti
Addì 11 aprile 2011-04-14 Reg. n. 8 Fog. N. 84

7.2. 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'ammi-nistrazione 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 Certifi-cata 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 im-plementare 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 automatiz-zati: prot.dgsia.dog@giustiziacert.it.
3. Terminate le operazioni di censimento da parte del responsabile per i sistemi informativi automa-tizzati, 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 e-ventuali 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 ap-posito 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 libe-ro>.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 infor-matico.
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 inse-rito 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 Infor-mativo Interforze del Ministero dell'Interno, secondo le specifiche del Si-stema 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 sottoforma 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 operazio-ne, 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 Re-GIndE 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 informa-zioni 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 iden-tificativi 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 inte-ressato (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 automa-tizzati 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 automa-tizzati, 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 ge-stita 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 qua-lificata 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 compo-nenti 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 sog-getti 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 Amministrazio-ne (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 anchesvolge-re 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 elet-tronica 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 telema-tici) 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 domi-nio giustizia è configurato un sottosistema per la memorizzazione e gestio-ne 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 pos-sono consultare sul portale dei servizi telematici, previa identificazione informatica di cui all'articolo 6, le informazioni relative ai pagamenti conte-nute 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)

Capitolo IX
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.

Mi sia consentita una considerazione finale, sicuramente impopolare e che non troverà il consenso di tutti i lettori.
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'inno-vazione 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, alterna-tivamente, 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)