CAMERA CIVILE DEGLI AVVOCATI

DELLA PROVINCIA DI GROSSETO

presenta

Guida Galattica per Giuristi Telematici

Guida teorico-pratica al processo civile telematico

Versione 1.1

Aggiornato al Provvedimento 16 aprile 2014

Luca Sileni

Sommario

Prefazione

Come referente informatico dell'Ordine degli Avvocati di Grosseto mi sono trovato, nel corso degli ultimi 4 anni, ad affrontare molte delle problematiche legate al processo civile telematico e, in particolare, alla difficile interazione tra il mondo dell'informatica e quello del diritto.

L'Avvocato di oggi è un giurista molto spesso poco informatizzato che utilizza il computer soprattutto quale sostituto moderno di carta e penna o, al massimo, di carta e macchina da scrivere.

Proprio dalle difficoltà – sperimentate da molti Colleghi – nella "digestione" dell'informatica applicata al diritto è nata l'idea di una "Guida galattica per giuristi telematici" che, parafrasando il noto romanzo di Douglas Adams, non vuol essere altro se non una guida "turistica" per l'Avvocato che si affacci all'alieno universo dell'informatica.

Questo e-book, quindi, avrà un taglio prettamente pratico senza però tralasciare le numerose problematiche di natura giuridica che si sono già manifestate in quasi un decennio di sperimentazione.

Oltre a ciò, sfruttando le peculiarità di proprie di un testo elettronico, cercherò di rilasciare periodicamente aggiornamenti e correzioni, sperando così di mantenere intatta l'utilità della guida.

CAPITOLO 1 – Cosa cambierà dopo il 30 giugno 2014

Paragrafo 1.1 – I riferimenti normativi

Preliminarmente ad ogni analisi relativa alle specifiche del processo civile telematico è necessario un breve riferimento ai principali testi normativi in ambito di PCT.

Deve *in primis* essere citato il Decreto Ministeriale 44/2011 (del quale – unitamente agli altri principali testi normativi in materia – è riportata una riproduzione integrale in calce a questa guida) che rappresenta il testo base in ambito di processo civile digitale.

La norma si occupa di definire le modalità e le procedure di trasmissione degli atti e dei documenti telematici agli Uffici Giudiziari, nonché di tutte le comunicazioni digitali che intercorrono fra i principali attori del processo civile e penale (notificazioni, comunicazioni dei biglietti di cancelleria, etc….)

Accanto al suddetto Decreto Ministeriale deve poi essere citato il c.d. "Provvedimento 16 aprile 2014 specifiche tecniche previste dall'articolo 34, comma 1 del decreto del Ministro della giustizia in data 21 febbraio 2011 n. 44" che ha recentemente sostituito il "Provvedimento 18 luglio 2011" e che nient'altro è se non un provvedimento attuativo del D.M. 44/2011 contenente, quindi, tutta una serie di indicazioni tecniche relative all'attuazione della normativa sulla trasmissione e sul deposito degli atti e dei documenti digitali.

Deve poi essere citata la L. 24 dicembre 2012, n. 228 (legge di stabilità 2013) oramai conosciuta anche dai non addetti ai lavori poiché accoglie, fra i suoi numerosi comma,

l'obbligo di deposito digitale – a partire dal 30 giugno 2014 – degli atti processuali e dei documenti allegati da parte dei Difensori già precedentemente costituiti[1].

Oltre a testi specificatamente afferenti al mondo del processo civile telematico, deve poi essere segnalato il Codice dell'Amministrazione Digitale – così detto CAD – ossia il Decreto Legislativo 7 marzo 2005, n. 82.

Tale testo normativo, lungi dall'essere una mera raccolta di norme indirizzate alle amministrazioni pubbliche, riunisce una moltitudine di definizioni e principi base dai quali il giurista telematico non può in alcun modo prescindere.

In detto testo, ad esempio, potremo ritrovare il diverso valore probatorio che l'Ordinamento conferisce alla firma elettronica semplice, alla firma elettronica qualificata e, infine, alla firma elettronica avanzata, oppure il valore legale conferito alla PEC.

Concetti che, comunque, verranno meglio chiariti nel prosieguo della trattazione.

Va infine ricordato, in materia di firma digitale, il Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013, recante le regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali. Testo di non facilissima lettura per il giurista poco informatizzato ma che, in ogni caso, reca con se importanti informazioni in ordine alla firma digitale.

[1] art. 1 comma 19 L. 24 dicembre 2012, n. 228

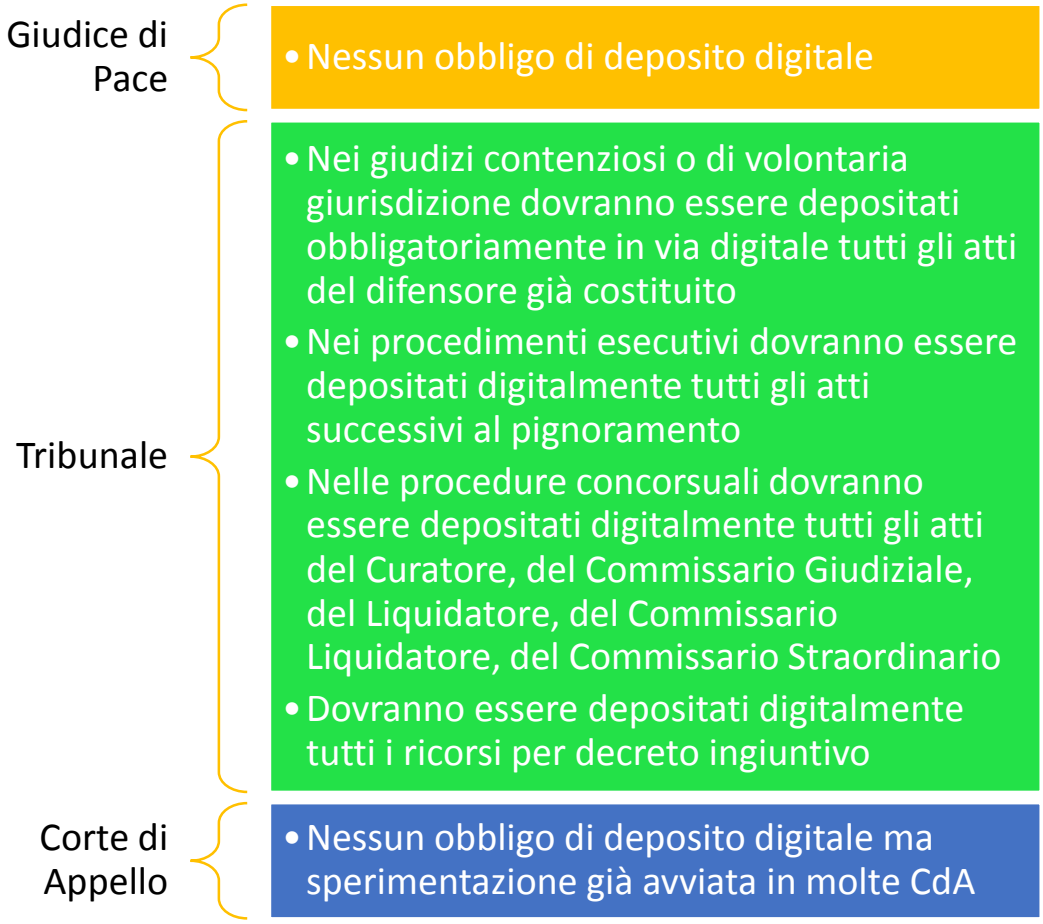
Paragrafo 1.2 – L'obbligo di deposito in digitale

Come è stato appena ricordato, a partire dal 30 giugno 2014 "*nei procedimenti civili, contenziosi o di volontaria giurisdizione, innanzi al tribunale, il deposito degli atti processuali e dei documenti da parte dei difensori delle parti precedentemente costituite ha luogo esclusivamente con modalità telematiche, nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici."* (legge di stabilità 2013).

L'obbligatorietà del deposito telematico è estesa poi – sempre dalla medesima norma – ai procedimenti monitori, alle procedure esecutive (con l'eccezione dell'atto di pignoramento) e alle procedure concorsuali (già parzialmente telematizzate a seguito della riforma della legge fallimentare).

A partire dal 30 giugno 2014 dovremo quindi obbligatoriamente depositare, in forma digitale, tutti gli atti civili successivi alla costituzione in giudizio, quali, ad esempio, le memorie 183 e le comparse conclusionali, restando pertanto escluso l'atto di citazione (e più in generale gli atti introduttivi del giudizio) e la comparsa di costituzione e risposta che però potrà comunque essere depositata digitalmente, benché non in via obbligatoria, in tutti i Tribunale che abbiano richiesto la specifica sperimentazione e che siano quindi abilitati alla ricezione.

Agli atti di cui sopra si aggiungeranno poi tutti i ricorsi per decreto ingiuntivo depositati dinanzi al Tribunale (ricordo che per adesso i Giudici di Pace sono esclusi dal procedimento di digitalizzazione dei fascicoli – v. schema seguente) e gli atti da depositarsi nelle procedure esecutive.



Lo schema che precede, però, indica unicamente quali saranno i cambiamenti a partire dal 30 giugno 2014, ma non cosa possa essere depositato digitalmente in via generale. Chiarisco, infatti, che la sperimentazione sul PCT sta comunque progredendo e molti Uffici Giudiziari hanno già avviato progetti sperimentali per il deposito di ulteriori atti di parte.

Il Tribunale di Torino, ad esempio, ammette il deposito con valore legale dei ricorsi ex art. 317 bis c.c[2], mentre il Tribunale di Tempio Pausania consente quello delle comparse di costituzione e risposta[3].

Allo stesso modo, pur non vigendo alcun obbligo di deposito digitale a decorrere dal 30 giugno p.v., alcune CdA hanno già provveduto ad avviare sperimentazioni telematiche, quali – ad esempio – la Corte di Appello di Salerno che, dal 15 aprile 2014, accetta con pieno valore legale le comparse di costituzione, di intervento e conclusionali nei procedimenti contenzioni, di volontaria giurisdizione e di lavoro[4].

Per rimanere sempre aggiornati sulle sperimentazioni in corso e per avere la certezza che un determinato atto sia ricevibile da un determinato Ufficio Giudiziario, consiglio di utilizzare l'apposita sezione del Portale dei Servizi Telematici del Ministero della Giustizia[5]

Tornando sull'obblio di deposito, però, la legge di stabilità 2013, oltre a dirci "cosa" dovremo obbligatoriamente depositare in via telematica dopo il 30 giugno 2014, ci ricorda anche "come" dovremo farlo, ossia, *"….nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici…."* richiamando, quindi, il Decreto Ministeriale 44/2011, il CAD e gli altri specifici provvedimenti attuativi che abbiamo citato nel paragrafo precedente.

---

[2] Decreto di avvio della sperimentazione sul PCT del Tribunale di Torino https://pst.giustizia.it/PST/do/ufficiepda/uffici/ricerca/downloadDecreto.action?idServiziAtti=444&fileName=DecretoAvvioPCTTorinoAttiparteLavoro.tiff

[3] Decreto di avvio della sperimentazione sul PCT del Tribunale di Tempio Pausania http://www.tribunaletempiopausania.it/allegati_sito/decreto_DGSIA_avvio_valore_legale_PCT.pdf

[4] Decreto avvio PCT della Corte i Appello di Salerno https://pst.giustizia.it/PST/do/ufficiepda/uffici/ricerca/downloadDecreto.action?idServiziAtti=830&fileName=DecretoAvvioPCTCASalernoAttiCCLavVG.tif

[5] Portale dei Servizi Telematici del Ministero della Giustizia https://pst.giustizia.it/PST/it/pst_2_4.wp

Se antecedentemente all'introduzione del PCT l'unica forma di deposito degli atti di causa era quella analogica (ossia cartacea), con l'avvento delle tecnologie digitali all'interno del processo civile il legislatore ha dovuto fare i conti con molte problematiche, sia di ordine pratico che di ordine giuridico, che via via si sono manifestate.

Nessun problema, infatti, vi era con la sottoscrizione analogica degli atti, posto che (per dirla con una battuta) al cambiare della penna utilizzata per la sottoscrizione certamente non sarebbe mutata la valenza della firma.

Nell'ambito delle sottoscrizioni digitali, invece, esistevano (ed esistono) una pluralità di "firme elettroniche" cui la legge – in particolare il CAD – conferiscono diverso valore giuridico.

Per la sottoscrizione degli atti digitali il legislatore ha scelto di adottare la c.d. "firma digitale", una particolare tipologia di firma elettronica avanzata che garantisce particolari standard di sicurezza sull'identificabilità – in modo univoco – del soggetto firmatario.

Accanto all'indicazione su quale tipologia di firma elettronica utilizzare nel processo civile telematico, però, la normativa si occupa anche di definire i formati – o se vogliamo gli standard specifici – da utilizzare nel PCT, ossia, il CADES-BES (identificato dall'estensione .P7M) [6] e il PADES-BES (utilizzabile per la sottoscrizione di soli file in formato pdf).

Tali formati non sono gli unici esistenti in ambito di firma digitale, ne esiste infatti un altro riconosciuto dal nostro Ordinamento, lo XADES, che è utilizzato per finalità diverse dalla firma dei documenti per il processo civile telematico.

[6] Cfr. Provvedimento 16 aprile 2014 - Art. 12 Formato dell'atto del processo in forma di documento informatico

A prescrivere l'uso del CADES-BES e del PADES-BES come unici formati idonei al deposito degli atti per via telematica è il "Provvedimento 16 aprile 2014" che innovando rispetto alla disciplina prevista dal "Provvedimento 18 luglio 2011" ha ammesso l'utilizzo del formato PADES-BES nel processo civile telematico (antecedentemente al 15 maggio 2014 – data di entrata in vigore del provvedimento 16 aprile 2014 – l'unico formato di firma digitale utilizzabile nel PCT era il CADES).

L'art. 12 del provvedimento 16 aprile 2014 prescrive *"La struttura del documento firmato è PAdES-BES (o PAdES Part 3) o CAdES-BES; il certificato di firma è inserito nella busta crittografica; è fatto divieto di inserire nella busta crittografica le informazioni di revoca riguardanti il certificato del firmatario. 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; nel caso del formato CAdES 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."*

Questo importantissimo articolo reca con se molte altre informazioni importanti delle quali ci occuperemo specificatamente nei capitoli seguenti.

Stabilito quale sia il formato che gli atti da depositarsi dovranno avere, dobbiamo già da adesso chiarire come dovremo procedere al perfezionamento delle operazioni di deposito.

Antecedentemente all'entrata in vigore del D.M. 44/2011, l'Avvocato telematico aveva l'obbligo di iscriversi ad un così detto PDA (punto di accesso) che si occupava di gestire,

per il professionista, le attività di invio degli atti telematici e di ricezione di comunicazioni e ricevute.

Questa attività veniva espletata attraverso un indirizzo PEC (CPE-CPT) interno al PDA creato *ad hoc*.

Con l'introduzione della normativa attuale, invece, l'Avvocato non è più obbligato a iscriversi a un PDA (che resta comunque un comodo metodo per gestire il PCT e per consultare i registri di cancelleria) ma gli basterà essere titolare di un indirizzo PEC funzionante, e procedere all'invio della busta elettronica crittografata (realizzata con apposito software di redazione) attraverso la propria posta elettronica certificata.

Il messaggio PEC dovrà avere, quale dimensione massima, 30 mb[7] e dovrà essere inoltrato entro le ore 14.00 [8] dell'eventuale giorno di scadenza per il deposito (sul punto è intervenuta una recente pronuncia del Tribunale di Milano, alla cui analisi – cfr. sottoparagrafo. 4.3.1 – rimando)

[7] Cfr. Provvedimento 16 aprile 2014 – Art. 14 Trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati – art 13 del regolamento

[8] Cfr. Decreto Ministeriale 44/2011 - Art.13 Trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati

CAPITOLO 2 – Lo Studio Legale Digitale

Paragrafo 2.1 - Gli strumenti di base per il PCT

Parlando con Colleghi, anche di altri distretti, mi sono reso conto dell'assoluta disinformazione che regna in ambito di strumenti necessari alla fruizione del PCT e, in particolare, in ordine ai costi degli strumenti *de quo*.

Come è logico che sia, le maggiori società operanti in ambito di editoria giuridica si sono buttate a capofitto nel mercato legato ai servizi telematici, sfruttando soprattutto quello che era l'assetto normativo antecedente al 2011.

Prima del D.M. 44/2011, come appena ricordato, vigeva per l'Avvocato l'obbligo di iscriversi ad un così detto PDA (acronimo di Punto di Accesso) per poter depositare atti e consultare i registri di cancelleria.

Con l'approvazione del sopracitato decreto, invece, si è sostanzialmente abbandonato l'obbligo di adesione ad un PDA dando la possibilità al professionista di operare in piena libertà nell'ambito del processo civile telematico.

Alla luce del fatto che, anche in virtù della contingenza economica attuale, è sempre più difficile far quadrare i conti di uno studio legale, cercheremo di capire quali siano gli strumenti necessari di cui l'Avvocato telematico non può fare a meno, come questi strumenti funzionino e quali siano i costi minimi da sostenere per il loro acquisto.

Sottoparagrafo 2.1.1 – La firma digitale

Il primo strumento di cui l'Avvocato telematico non potrà più fare a meno è la firma digitale.

Il CAD definisce la firma digitale *"un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici "*[9]; detto strumento, quindi, altro non sarà che un mezzo per manifestare, da un lato, e di verificare, dall'altro, la provenienza di un determinato documento informatico.

Il CAD, però, fa *in primis* un'importante distinzione fra le varie tipologie di firma elettronica e, in particolare, fra

- Firma elettronica (c.d. "semplice") *l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;*[10]
- Firma elettronica avanzata *insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo,*

[9] Cfr. art. 1 lettera s) Decreto Legislativo 7 marzo 2005 n° 82

[10] Cfr. art. 1 lettera q) Decreto Legislativo 7 marzo 2005 n° 82

collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati[11]

Per quanto attiene alla nostra analisi, non potendoci – in questa sede – addentrare ulteriormente nell'analisi delle varie tipologie di firma, è importante sapere che la c.d. firma elettronica semplice altro non è se non un insieme di dati utilizzati per il riconoscimento "di base" di un determinato soggetto e quindi, ad esempio, il classico nome utente e password che utilizziamo per accedere alla nostra posta elettronica, oppure il pin utilizzato per il bancomat, etc…. Tale tipologia di autenticazione, quindi, viene comunemente definita "debole" in virtù dell'estrema facilità di manipolazione dei dati *de quo*.

La firma elettronica avanzata (di cui la firma elettronica qualificata e la firma digitale sono sottospecie) consente invece di garantire una connessione **univoca** al soggetto firmatario, e per tale ragione detta tipologia di autenticazione è definita "forte".

Tale distinzione riveste ancora più importanza per il giurista, se la si analizza alla luce del disposto dell'art. 20 del CAD [12], il quale chiarisce che solo i documenti sottoscritti con firma elettronica avanzata, qualificata o digitale, fanno piena prova, fino a querela di falso, ex art. 2702 c.c., mentre quelli sottoscritti con firma elettronica semplice saranno liberamente valutabili in giudizio.

Posto, quindi, che per la sottoscrizione di un atto digitale che dovesse sostituire in tutto e per tutto un documento cartaceo munito di sottoscrizione olografa, sarebbe necessario ricorrere ad uno strumento elettronico estremamente avanzato e in grado di attestare con

[11] Cfr. art. 1 lettera q-bis) Decreto Legislativo 7 marzo 2005 n° 82

[12] Cfr. art. 20 comma 2 Decreto Legislativo 7 marzo 2005 n° 82: *Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria."*

certezza l'attribuzione della firma sul documento, si comprende come mai il legislatore abbia sancito l'obbligatorietà – nel processo civile telematico – della firma digitale.

Chiarito, anche se con un'analisi superficiale, che cosa sia in astratto una firma digitale, cercheremo ora di capire da che cosa – in concreto – tale firma sia rappresentata e quali siano gli usi che il giurista telematico può farne.

I dispositivi di firma digitale possono essere di varia tipologia (smart card, chiavetta USB, token, etc…) e solitamente hanno un costo variabile dai 50 ai 110 euro.

Per esperienza personale consiglio a tutti i Colleghi di dotarsi di una firma digitale su supporto USB, molto più pratica da utilizzare e che non necessita di un lettore di smart card da installare sul proprio computer di studio.

Indipendentemente dalla tipologia di dispositivo scelto, il kit di firma digitale ci permetterà di sottoscrivere, con piena validità legale, non solo il nostro atto digitale da depositare in Tribunale, ma anche missive, atti da notificarsi in proprio e, più in generale, documenti informatici.

Detta sottoscrizione potrà essere apposta con una pluralità di formati di firma digitale, fra cui, i più conosciuti ed utilizzati, sono il PADES e il CADES (tralasciamo, in questa sede, l'analisi del formato XADES poiché di raro utilizzo nella pratica forense).

Il PADES (PDF Advanced Electronic Signature o più comunemente "firma in pdf")[13] rappresenta uno dei formati più diffusi in ambito professionale e ha la peculiarità di permettere la creazione – assieme al codice digitale che rappresenta la vera e propria firma

[13] Il formato è riconosciuto in virtù del disposto dell'art. 21 n° 15 della deliberazione CNIPA 45/2009: *"Ai sensi del comma 8, con la presente deliberazione, sono riconosciuti il formato di busta crittografica e di firma descritti nello standard ISO/IEC 32000 – Portable Document Format (PDF) sviluppati in conformità alle specifiche ETSI TS 102 778 - PAdES."*

digitale – anche di una sottoscrizione "per immagine" da apporre direttamente sul documento che si va a firmare.

Un file PDF sottoscritto in formato PADES, quindi, oltre a non venire modificato nella sua struttura (il file firmato rimarrà comunque un PDF) potrà essere accompagnato da una visualizzazione grafica della firma digitale che, invece, è solitamente assente nei documenti sottoscritti in formato CADES.

Tale tipologia di sottoscrizione è largamente impiegata per le comunicazioni fra Colleghi e, a seguito delle innovazioni introdotte dal "Provvedimento 16 aprile 2014", anche per le attività di sottoscrizione di atti digitali.

Il PADES, infatti, ha l'indubbio vantaggio della versatilità e della facilità di utilizzo, poiché, non modificando il formato finale del file firmato (che rimarrà un classico PDF), sarà accessibile e consultabile con un semplice "doppio click" sull'icona del file, senza necessità di attività particolari volte alla verifica della firma.

Attività che, comunque, sono consigliabili per avere certezza dell'avvenuta sottoscrizione e della validità della sottoscrizione stessa.

Il sistema CADES (CMS Advanced Electronic Signature)[14], contrariamente al formato appena analizzato, inserisce il documento originale (poniamo ad esempio il file atto.pdf) all'interno di una busta virtuale che viene sottoscritta digitalmente, mutando l'estensione del file originale (che diverrà atto.pdf.p7m) e lasciando tale firma invisibile.

Per il controllo della firma sul documento sarà quindi necessario avvalersi di un apposito software di supporto che, oltre a verificare la sottoscrizione e la validità della stessa, permetta anche l'apertura della busta digitale, rendendo quindi accessibile il documento nella stessa contenuto.

[14] Il formato è riconosciuto in virtù del disposto dell'art. 21 n° 1 e ss. della deliberazione CNIPA 45/2009:

Il CADES (o come da molti chiamato “P7M”) è quindi, per una buona parte dei Colleghi, uno strano essere digitale poco digeribile da parte dei nostri computer di studio, ciò perché l'apposizione della firma in CADES, come sopra accennato, comporta la modificazione del formato del file che stiamo firmando.

La firma, di fatto, non viene infatti posta direttamente sul file digitale ma su una busta all'interno della quale il nostro file viene inserito.

Il file finale risultante a seguito del processo di firma avrà denominazione: nomefileoriginale.estensioneoriginale.p7m.

Chi mastica un po' di informatica sa che le ultime lettere che troviamo, dopo il punto, in quasi tutti i file presenti sul nostro computer, non sono altro che un'indicazione data al sistema operativo, volta a far comprendere a quest'ultimo con quale programma dovrà aprire quella determinata tipologia di file.

Se quindi, riprendendo il nostro esempio di cui sopra, il file originario fosse "atto.pdf" il nostro computer saprà di doverlo aprire attraverso un classico lettore di file pdf (come il noto software “Acrobat Reader”), ma se il nostro file fosse invece stato inserito all'interno di una busta virtuale e denominato "atto.pdf.p7m" il computer non saprebbe più di doverlo aprire attraverso Acrobat Reader (o altro analogo software), non essendo più in grado di riconoscere quel file come un classico pdf.

A quel punto, quindi, sarà necessario avvalersi di un software che si occupi di verificare la validità della firma apposta sulla busta, nonché di aprire il file p7m permettendo la lettura dell'originario "atto.pdf".

La verifica potrà essere effettuata tramite il medesimo software che utilizziamo per la sottoscrizione dei documenti.

I Colleghi che siano in possesso di un kit di firma digitale su supporto USB, saranno in grado di effettuate la verifica *de quo* tramite il software preinstallato sulla chiavetta, mentre coloro che utilizzassero una smart card oppure una chiavetta USB priva di memoria fisica, potranno installare uno dei software di firma digitale gratuiti presenti in rete.

I più conosciuti ed utilizzati sono Aruba Sign[15] e Dike[16].

Detti programmi, a seguito della loro completa installazione, permetteranno, oltre all'apposizione della firma digitale su un qualsiasi documento, anche l'apertura diretta - con il classico "doppio click" - di tutti i file con estensione P7m.

Qualora, invece, non si volesse o non fosse possibile installare un software atto alla verifica della firma digitale, esiste la possibilità di procedere ad una verifica on line senza l'ausilio di applicativi esterni collegandosi ai portali:

- Infocert[17]
- Postecert[18]
- Notariato[19]

[15] Scaricabile all'indirizzo: http://www.pec.it/Download.aspx

[16] Scaricabile all'indirizzo: https://www.firma.infocert.it/installazione/installazione_DiKe.php

[17] Pagina di verifica infocert https://www.firma.infocert.it/utenti/verifica.php

[18] Pagina di verifica sul sito di Poste Italiane https://postecert.poste.it/verificatore/servletverificatorep7m?tipoOp=10

[19] Pagina di verifica del notariato http://vol.ca.notariato.it/

Sottoparagrafo 2.1.2. – La posta elettronica certificata

Secondo strumento indispensabile all'attività professionale del giurista digitale, è poi la posta elettronica certificata (PEC). Strumento divenuto oramai di uso comune in molti ambiti professionali ed obbligatoria per tutti gli Avvocati già dal 2009.

Il costo medio annuo si aggira sui 4 euro, ma la stragrande maggioranza degli ordini professionali ha provveduto a fornirla gratuitamente ai propri iscritti.

La Posta Elettronica Certificata è definita, dall'art. 1 del DPR 11/02/2005 n. 68, *"sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi"*[20].

Da questa semplice definizione possiamo già facilmente comprendere in cosa consista quell'accezione "certificata" che differenzia la PEC da un normale sistema di posta elettronica, ossia, nell'attestazione digitale **esterna** dell'avvenuto invio e dell'avvenuta consegna di documenti informatici.

In pratica quindi, contrariamente ai normali sistemi di mail in cui il nostro messaggio attraversa la rete senza nessuna certezza sull'effettiva ricezione e senza nessuna reale coscienza su chi sia realmente il destinatario cui è indirizzata, la PEC ci consente di avere un'attestazione (fornita da un certificatore esterno abilitato) relativa a 4 elementi principali:

1) Indirizzo del mittente
2) Indirizzo del destinatario
3) Data di invio
4) Data di ricezione

[20] Cfr. art. 1 lettera v-bis del CAD

In virtù della certificazione di cui sopra, il DLT 07/03/2005 n. 82 (Codice dell'Amministrazione digitale) equipara – all'art. 48 comma II[21] – la comunicazione inviata tramite PEC ad una classica raccomandata A/R.

Se quindi il nostro indirizzo di posta elettronica certificata (di cui – ex art. 16 comma 7 D.L. 185/2008[22] – tutti gli Avvocati devono essere dotati) è mezzo idoneo a sostituire la raccomandata A/R, quali potranno essere gli utilizzi che il professionista digitale potrà farne?

Decisamente molteplici!

Partiamo innanzitutto dal presupposto che – ad oggi – sussiste un obbligo di dotarsi di un indirizzo di posta elettronica certificata per:

a) Ditte individuali

b) Società

c) Alcune categorie di professionisti (fra cui gli Avvocati)

d) Pubbliche amministrazioni

con tutta evidenza, quindi, le normali comunicazioni con i soggetti di cui sopra, potranno essere effettuate tranquillamente via PEC invece che con i classici sistemi analogici.

Potremo quindi effettuare via PEC:

A) gli scambi di fax con i Colleghi, risparmiando su carta, toner e costo della telefonata;

B) la messa in mora o la richiesta di adempimento rivolta ad una qualsiasi società o ditta individuale, con notevole risparmio sul costo della raccomandata;

---

[21] Cfr. art. 48 comma II del CAD *"La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta."*

[22] Cfr. art. 16, comma 7, D.L. 185/2008 "*I professionisti iscritti in albi ed elenchi istituiti con legge dello Stato comunicano ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata ((o analogo indirizzo di posta elettronica di cui al comma 6)) entro un anno dalla data di entrata in vigore ((del presente decreto…*"

C) l'insinuazione al passivo nelle procedure fallimentari (in questo caso parliamo di un obbligo e non di una facoltà, prescritto dalla nuova formulazione dell'art. 93 L.F.)[23];

D) le notificazioni in proprio previste dalla L. 53/94 (facoltà espressamente concessa dall'art. 3-bis della medesima legge), anche in questo caso con notevole risparmio sulle spese postali e di notifica;

E) il deposito degli atti endoprocessuali – nei procedimenti civili ordinari – ed i ricorsi per decreto ingiuntivo. Per tali tipologie di documento – come abbiamo già visto – sussiste l'obbligo di deposito tramite PEC a partire dal 30 giungo 2014.

Lasciando ai seguenti capitoli l'esame del deposito dell'atto processuale telematico, vediamo come è possibile approntare una comunicazione via PEC che sostituisca in tutto e per tutto un fax o una raccomandata.

Preliminarmente ad ogni ulteriore indicazione vi è innanzitutto da rispondere al quesito che molti lettori potrebbero già essersi posti, ossia, "dove trovo l'indirizzo PEC del destinatario?"

La risposta varia a seconda della tipologia di destinatario che si stia ricercando.

Attualmente esistono più registri PEC attivi in Italia, ed esempio, il ReGIndE che racchiude le PEC dei soggetti esterni abilitati al PCT, come i CTU o gli Avvocati, oppure il registro della camera di commercio che reca gli indirizzi di società e ditte individuali, ma – per nostra comodità – basterà far riferimento a due indici generali di riferimento:

[23] Art. 93 comma II Legge Fallimentare: *"Il ricorso può essere sottoscritto anche personalmente dalla parte ed è formato ai sensi degli articoli 21, comma 2, ovvero 22, comma 3, del decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni e, nel termine stabilito dal primo comma, è trasmesso all'indirizzo di posta elettronica certificata del curatore indicato nell'avviso di cui all'articolo 92, unitamente ai documenti di cui al successivo sesto comma. L'originale del titolo di credito allegato al ricorso è depositato presso la cancelleria del tribunale"*

1) il registro INI PEC – che racchiude gli indirizzi di posta elettronica dei professionisti che abbiano l'obbligo di dotarsi di un indirizzo di posta certificata, di tutte le imprese individuali e di tutte le società;[24]

2) Il registro IPA – che raccoglie, invece, gli indirizzi PEC delle pubbliche amministrazioni;[25]

Accedendo, quindi, alle pagine web dei due indici sopra richiamati, potremo – ad esempio – scovare la PEC del Collega a cui volevamo inviare una comunicazione, oppure dell'azienda a cui dobbiamo recapitare una messa in mora.

Una volta individuato l'indirizzo PEC del destinatario possiamo quindi procedere all'elaborazione della nostra comunicazione e al suo invio.

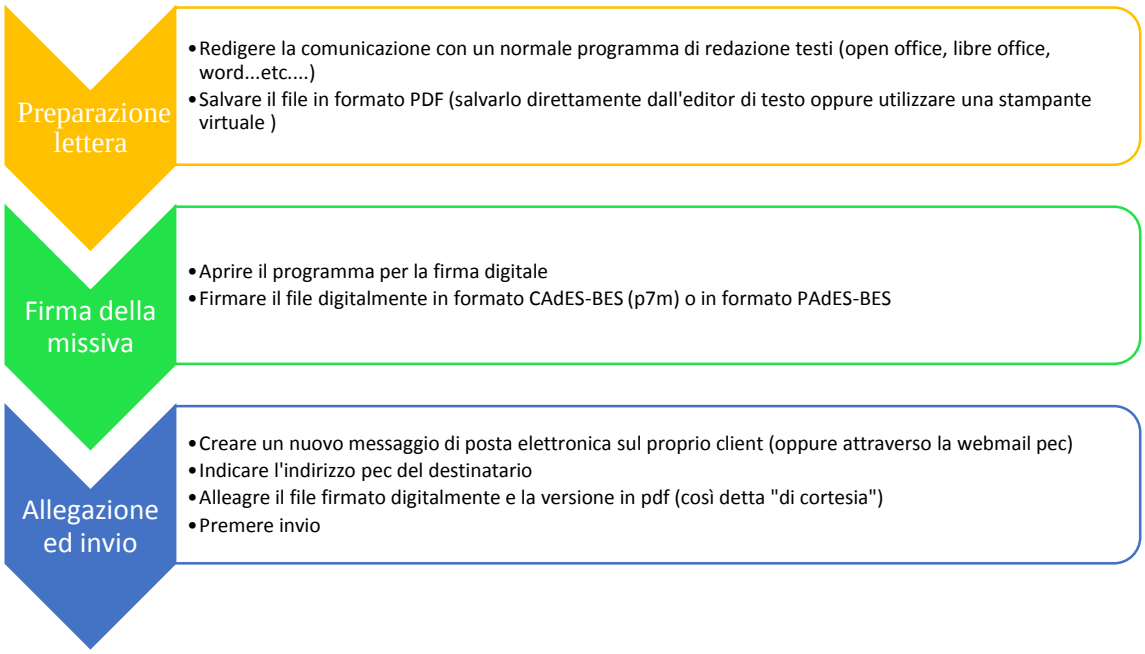
Normalmente quando inviamo un messaggio di posta elettronica inseriamo il testo del messaggio nel corpo dell'email, nella redazione di un messaggio PEC, invece, procederemo diversamente.

Le ragioni di questa diversa procedura saranno meglio chiarite nella parte finale di questo paragrafo.

Vediamo ora di capire, quindi, quali siano le fasi principali della preparazione e dell'invio del nostro messaggio PEC attraverso lo schema che segue.

[24] Il registro è consultabile all'indirizzo https://www.inipec.gov.it/

[25] Il registro è consultabile all'indirizzo http://www.indicepa.gov.it/documentale/index.php



Per la fase di "preparazione" avremo semplicemente bisogno del nostro classico editor di testo (open office, word…. etc…..) per redigere la missiva, avendo cura, una volta completata la procedura di scrittura, di salvarla in formato pdf.

La maggior parte degli editor di testo di ultima generazione (approssimativamente tutte le versioni successive al 2007) permettono l'esportazione o il salvataggio diretto dei file in formato pdf, qualora – però – il vostro programma non consentisse questa facoltà, le alternative possono essere due:

1) Scaricare e installare una stampante virtuale in pdf, ossia, un programma che crei una stampante residente sul vostro pc che – in realtà – nulla ha di fisico, ma che si limiti a salvare un nuovo file in formato pdf.

2) Acquistare una nuova versione del vostro programma di video scrittura, o scaricare gratuitamente editor open source quali open office[26] o libre office[27].

Una volta salvata una copia pdf della vostra missiva potrete passare alla fase di sottoscrizione.

Come detto nel precedente paragrafo, la maggior parte dei supporti di firma digitale vengono forniti con il proprio software a corredo e quindi con tutto il necessario per poter firmare un file digitalmente.

Qualora la vostra smart card, chiavetta USB per firma digitale o altro supporto di firma, non fosse stato invece venduto unitamente ad un programma per la sottoscrizione digitale, non vi rimarrà che scaricare e installare – gratuitamente – uno dei due programmi di firma maggiormente diffusi: Arubasign[28] oppure Dike[29].

Dopo aver aperto il programma per la sottoscrizione digitale, non dovrete far altro che caricare – dall'applicativo – il file pdf da firmare, selezionare il formato di firma (andranno bene sia il formato CADES-BES – *alias* P7M – sia il formato PADES-BES) ed inserire il pin o la password.

Giunti, poi, all'ultima fase del processo di preparazione e invio del nostro messaggio di PEC non avremo che da aprire il client di posta elettronica installato sul nostro computer (outlook, thunderbird, mail, windows mail… etc…..) e creare un nuovo messaggio.

[26] http://www.openoffice.org/it/

[27] http://it.libreoffice.org/

[28] Scaricabile all'indirizzo: http://www.pec.it/Download.aspx

[29] Scaricabile all'indirizzo: https://www.firma.infocert.it/installazione/installazione_DiKe.php

Per gli utenti che utilizzassero thunderbird come client di posta predefinito, consiglio di utilizzare il formato PADES-BES per la sottoscrizione dei documenti digitali, ciò in virtù dell'incapacità di detto software di gestire nativamente i file .p7m come allegati ai messaggi di posta elettronica.

Raccomando, poi, di fare sempre molta attenzione alla selezione del mittente perché, qualora aveste configurato più indirizzi di posta elettronica sul client mail, il programma utilizzerà in automatico l'indirizzo di posta predefinito e non necessariamente quello di PEC.

Onde evitare errori, quindi, l'indirizzo mittente andrà selezionato come prima operazione successiva alla creazione del messaggio di posta.

Fatto ciò non ci resterà che scrivere l'indirizzo del destinatario, allegare il file firmato digitalmente, allegare la missiva non sottoscritta in formato pdf (come copia di cortesia nel caso utilizzaste il formato CADES-BES per la sottoscrizione del file digitale) e premere invio.

Il corpo della mail potrà essere lasciato in bianco oppure – a seconda del tipo di comunicazione – potrà riportare diciture quali "In allegato troverà la missiva firmata digitalmente".

In merito al perché si opti per questa procedura – invero un po' macchinosa – per redigere ed inviare un messaggio PEC, dobbiamo tenere presente quale sia il valore che vogliamo conferire alla nostra comunicazione veicolata tramite la posta elettronica certificata, ossia, quello di una raccomandata.

Se, come abbiamo detto, la PEC attesta: indirizzo mittente, indirizzo destinatario, ora di invio ed ora di ricezione, per far sì che il contenuto sia sottoscritto in modo analogo ad una normale lettera raccomandata, dovremo obbligatoriamente redigere la nostra missiva

in formato elettronico (con il programma di video scrittura) e firmarla digitalmente, inserendola poi, quale allegato, nel messaggio di posta elettronica certificata.

Sostanzialmente, con questa procedura, non faremo altro che utilizzare la PEC quale vettore per trasmettere il messaggio allegato, un po' come se il messaggio di posta elettronica certificata non fosse altro che la classica busta bianca all'interno della quale inseriamo la nostra comunicazione inviata per raccomandata.

Senza addentrarci eccessivamente in argomenti che sono oggetto di continue modifiche normative e difettano ancora di un sufficiente numero di pronunce giurisprudenziali, è necessario però sottolineare che la comunicazione via PEC, redatta nel corpo della mail e non inserita come allegato sottoscritto digitalmente, non sia comunque da considerarsi priva di alcuna sottoscrizione.

Da un lato, infatti, alla PEC (e quindi al testo presente nel corpo del messaggio di posta) è stato inizialmente conferito il rango di "firma elettronica semplice" che, come abbiamo sottolineato nel paragrafo precedente, *"è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità."* [30]

Dall'altro, a seguito di recenti interventi normativi, è stato stabilito che l'invio tramite posta elettronica certificata di cui all'articolo 65, comma 1, lettera c-bis) del Codice dell'Amministrazione Digitale, sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata.[31]

[30] Cfr. art. 21 del CAD

[31] Cfr. art. 65 lett. C-bis del CAD *"ovvero se trasmesse dall'autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce dichiarazione vincolante ai sensi dell'articolo 6, comma 1, secondo periodo. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario"*

In questo modo, il semplice invio tramite PEC – senza ulteriore sottoscrizione elettronica – è stato (esclusivamente nei casi in cui il messaggio sia rivolto ad una pubblica amministrazione) equiparato alla firma elettronica avanzata.

Se da un lato, però, il legislatore apre le porte ad una sorta di "sottoscrizione automatica" delle PEC nei confronti della PA, dall'altro – in preda alla solita schizofrenia propria del normatore italico – limita l'equiparazione alla firma elettronica avanzata, del messaggio di posta certificata, unicamente ai casi di utilizzo di una PEC-ID[32], ossia, di un indirizzo PEC il cui certificatore funga anche da "identificatore" del mittente, ed abbia provveduto ad accertare l'identità di quest'ultimo attraverso, ad esempio, l'esibizione fisica di un documento di identità oppure attraverso la sottoscrizione digitale (e quindi facendo tornare in auge la necessità di una firma digitale) di un modulo di adesione (per gli altri metodi di identificazione si rimanda alla lettura degli artt. 5 e 6 del DPCM 27 settembre 2012[33]).

---

[32] Per le regole tecniche, le modalità di rilascio ed identificazione si veda il DPCM 27 settembre 2012 alla nota seguente.

[33] DPCM 27 settembre 2012 - Art. 5 "*1. Le operazioni di identificazione del Titolare sono curate dal Gestore nell'ambito delle attività e delle funzioni per la registrazione di cui all'art. 21, comma 1, lettera a) del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005.*
2. L'identificazione di cui all'art. 65, comma 1, lettera c-bis) del CAD avviene, in occasione di ogni attribuzione di credenziali di accesso, in uno dei seguenti modi:
a) mediante la sottoscrizione del modulo di adesione al servizio di cui all'art. 65, comma 1, lettera c-bis) del CAD ed esibizione al Gestore, da parte del Titolare, di un valido documento d'identità e del codice fiscale;
b) tramite la compilazione del modulo di adesione disponibile in rete, previa identificazione informatica tramite CIE o CNS;
c) mediante la sottoscrizione con firma digitale, di cui all'art. 1, comma 1, lettera s) del CAD, del modulo di adesione al servizio di cui all'art. 65, comma 1, lettera c-bis) del CAD;
d) a mezzo di apparecchiature che utilizzino necessariamente una SIM/USIM dotate di codici PIN/PUK o loro evoluzioni tecnologiche rilasciate previa identificazione del titolare delle medesime nel rispetto delle disposizioni vigenti.
3. Il Gestore verifica la corrispondenza dei dati forniti dal Titolare con le generalità indicate nel documento d'identità o associate alla SIM/USIM e conserva la relativa documentazione per il periodo di durata del servizio PEC-ID e per un periodo pari a ventiquattro mesi successivi alla cessazione del servizio PEC_ID.
4. Nel modulo di adesione al servizio di cui all'art. 65, comma 1, lettera c-bis) del CAD il Titolare manifesta l'eventuale assenso di cui all'art. 6 del CAD".
Art. 6: *"1. Ai fini dell'identificazione per l'accesso al servizio PEC-ID, il Gestore predispone una delle seguenti modalita':*
a) identificazione tramite Certificato di autenticazione della CNS;

Cercando però di rientrare nei ranghi di una guida pratica, quale questa vuole essere, ed allontanandoci quindi da problemi di natura giuridica ancora poco dibattuti in dottrina e giurisprudenza, a noi basterà ricordare che: il messaggio di Posta Elettronica Certificata realizzato con le modalità sopra descritte, può andare a sostituire, in tutto e per tutto, una classica lettera raccomandata e potrà quindi essere utilizzata non solo per l'invio della busta telematica da depositare in Tribunale ma anche per effettuare le notificazioni in proprio, per inviare l'istanza di insinuazione al passivo al curatore fallimentare o, più semplicemente, per inoltrare intimare un pagamento.

A tal riguardo, però, è infine necessario ricordare che la facoltà di notificazione via PEC è ammessa – ad oggi – esclusivamente in materia civile, amministrativa e stragiudiziale (così come previsto dall'art. 1 della L. 53/1994) ed è invece esclusa – almeno per il momento – in materia tributaria e penale (come recentemente stabilito anche dal Tribunale di Roma[34][35])

Sottoparagrafo 2.1.3. – Il redattore atti

Il c.d. "redattore atti" altro non è che il programma di cui dovremo servirci per l'elaborazione della busta digitale da depositare telematicamente.

b) identificazione tramite Certificato di autenticazione della CIE;
c) identificazione tramite credenziali di accesso basate su identificativo-utente, parola d'ordine (password) e parola d'ordine temporanea (one time password) trasmessa attraverso sistemi di telefonia mobile;
d) identificazione tramite credenziali di accesso basate su identificativo-utente, parola d'ordine (password) e parola d'ordine temporanea (one time password) generata dal token crittografico rilasciato dal Gestore medesimo."

[34] Per approfondimenti si consiglia la consultazione dell'articolo: "premesse generali sulle notifiche in proprio" dell'Avv. Juri Rudi: http://www.studiolegalerudi.it/pct/?page_id=266

[35] Si veda l'articolo: comunicazioni e notificazioni nel processo penale: http://salavvocatifrascati.tumblr.com/post/58903389464/comunicazioni-e-notificazioni-nel-processo-penale-la#.U2StSfl_vkM

Tale software si rende necessario per adempiere agli obblighi sanciti dall'art. 14 del "Provvedimento 16 aprile 2014"[36] che richiede l'inserimento di tutti i documenti da trasmettere alla Cancelleria del Tribunale all'interno di un unico file crittografato.

Appare chiaro che, in virtù della scelta ministeriale di non realizzare un proprio programma di redazione atti, il software necessario ad elaborare la busta telematica sia divenuto uno dei maggiori business delle società che operano nel settore dei servizi professionali a pagamento.

L'Avvocato telematico, quindi, sarebbe teoricamente costretto ad acquistare la licenza di uno dei vari programmi di redazioni presenti sul mercato, oppure decidere di dotarsi di un gestionale di ultima generazione che integri anche le funzionalità del PCT.

Essendo i software di cui sopra molto diversi l'uno dall'altro (soprattutto per moduli e funzionalità) in questa sede non si potrà effettuare un'analisi approfondita di tutte le soluzioni esistenti.

[36] *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. Tale file deve essere omesso qualora il suo contenuto sia presente nella sezione apposita del file DatiAtto.xml, come da XSD di cui al successivo punto b). b) DatiAtto.xml: gli XSD sono riportati nell'Allegato 5. c) <nome file (libero)>: atto vero e proprio, in formato PDF, sottoscritto con firma digitale o firma elettronica qualificata secondo la struttura dell'articolo 12 comma 2. d)AllegatoX.xxx: 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.*
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).

Posto però che, nel prosieguo della trattazione, sarà comunque necessario (anche a mero fine esemplificativo) riferirsi ad un programma per l'elaborazione della busta digitale, ritengo che, in questa sede, sia il caso di far menzione dell'applicativo " SLPCT".[37]

Tale scelta è determinata unicamente da ragioni di opportunità, il programma realizzato dalla Evoluzioni Software per la Regione Toscana, infatti, è l'unico – ad oggi e per quanto a conoscenza di chi scrive – rilasciato con licenza open source.

Detto programma, quindi, è gratuito e rimarrà tale anche in futuro.

In ogni caso segnalo che il Ministero ha dedicato una sezione – nel proprio portale dei servizi telematici – dedicata ai software *"free to use"* per la realizzazione della busta telematica.[38]

I programmi inseriti nella lista non sono tutti completamente gratuiti, quindi, per una scelta oculata del redattore, segnalo – in nota – due interessanti articoli, il primo dell'Avvocato Simone Aliprandi[39], il secondo pubblicato dall'Associazione Nazionale Forense di Roma.[40]

Sottoparagrafo 2.1.3. – Il punto di accesso

Come detto in precedenza non è più strettamente necessario munirsi di un punto di accesso per poter depositare telematicamente le buste digitali, ma è indubbio come, l'accesso ad un portale di questo tipo, renda infinitamente più agevole la vita di un

[37] Il programma è scaricabile liberamente dal PDA Regione Toscana https://www.giustizia.toscana.it/cancelleriatelematica o, in alternativa dal *mirror* *http://www.sph3ra.it/redattore-gratuito-slpct/*

[38] https://pst.giustizia.it/PST/it/pst_28.wp

[39] http://aliprandi.blogspot.it/2014/03/software-processo-telematico.html

[40] https://www.facebook.com/ANF.SINDACATO.ROMA/posts/598177763610610

Avvocato, che - attraverso il proprio PDA - potrà consultare i registri di cancelleria di tutti i Tribunali d'Italia.

Esiste però la possibilità di ottenere il medesimo risultato senza far ricorso ai più o meno costosi servizi a pagamento presenti sul mercato, ossia, utilizzare le funzionalità del portale dei servizi telematici del ministero della giustizia.

Il così detto PST Giustizia [41], infatti, consente non solo la consultazione dei registri di cancelleria di tutti i Tribunali italiani, ma anche la possibilità di consultare il RegIndE (Registro Generale degli Indirizzi Elettronici), di effettuare pagamenti telematici (anche del contributo unificato) e di essere aggiornati su news ed eventuali disservizi relativi alle piattaforme dei sistemi ministeriali.

In conclusione, sul punto, pur rimanendo indubbia la comodità e versatilità dei gestionali di ultima generazione e dei PDA realizzati da molte società attive nell'ambito dei servizi ai professionisti dell'area legale (si precisa che anche i PDA "commerciali" consentono normalmente la consultazione gratuita dei registri di cancelleria), ciò non toglie che l'Avvocato telematico debba essere conscio che l'acquisto di detti servizi è assolutamente non obbligatorio per svolgere correttamente e proficuamente la professione.

Paragrafo 2.2 – Le 5 regole d'oro per sopravvivere al PCT

Stabiliti quali siano gli strumenti assolutamente indispensabili per il processo civile telematico è a questo punto necessario affrontare alcune problematiche di ordine pratico con le quali tutti i Colleghi dovranno fare i conti prima del 30 giugno 2014.

[41] http://pst.giustizia.it/PST/

Orientarsi nel mondo dell'informatica non è certo semplice per chi non ha dimestichezza con il mondo dei computer e della tecnologia in generale, ma per dirsi pronti all'avvento del PCT potranno bastare gli strumenti indispensabili visti al paragrafo precedente e le 5 semplici regole pratiche che seguono.

Sottoparagrafo 2.2.1 – L'uso dello scanner

Dando per scontato che chiunque di noi sappia che cos'è uno scanner, con l'avvento del PCT potrebbe non essere più sufficiente avere a disposizione un semplice scanner "piano".

Posto, infatti, che il nostro fascicolo dovrà diventare interamente digitalizzato, non sarà più pensabile continuare ad utilizzare un macchinario che scannerizza una pagina per volta.

Primo punto da soddisfare per essere pronti all'arrivo del processo civile telematico, quindi, sarà certamente l'acquisto di uno scanner con ADF.

L'ADF non è altro che un caricatore dall'alto che permette di inserire un intero documento (quindi formato anche da molti fogli) nel nostro strumento di acquisizione digitale, restituendo, alla fine, un unico file tiff o pdf.

Visto che anche per il semplice procedimento monitorio sarà necessario allegare documenti a volte formati da diverse decine di pagine, appare assolutamente indispensabile munirsi di uno strumento come questo.

Certamente, però, non basterà acquistarlo per essere pronti ad affrontare senza timori la digitalizzazione del processo civile, poiché condizione indispensabile sarà anche quella di imparare ad usarlo in modo oculato.

Come sappiamo, infatti, la busta telematica da inviare alla cancelleria del Tribunale per effettuare il deposito degli atti, non potrà avere dimensione superiore a 30 mb[42]. Questa dimensione, per la verità piuttosto esigua, verrà certamente superata se l'Avvocato telematico scannerizzerà i propri documenti alla massima risoluzione e, magari, addirittura a colori.

Per cercare di risparmiare quanto più spazio possibile, quindi, sarà assolutamente indispensabile imparare a gestire le impostazioni dello scanner settando la risoluzione a non più di 150 o 200 dpi e ricordandosi di scannerizzare (ove possibile) in bianco e nero. Impostare una risoluzione base di scannerizzazione piuttosto bassa ci permetterà di creare dei file di dimensioni ridotte e di ricorrere a qualità di scannerizzazione più alte solo qualora il file risulti di difficile lettura.

Sottoparagrafo 2.2.2 – L'organizzazione delle cartelle

Abbiamo appena visto che il nostro fascicolo, un tempo unicamente cartaceo, a partire dal 30 giugno p.v. diventerà completamente virtuale.

Ciò significa che il numero di file digitali legati ad una singola pratica aumenterà considerevolmente.

Se, per fare un esempio, un tempo il più classico recupero credito trovava posto sui nostri computer solo con la lettera di messa in mora e il ricorso per decreto ingiuntivo, con l'avvento del processo civile telematico dovremo avere sul nostro pc almeno:

a) Corrispondenza (es. messa in mora)

b) Ricorso per decreto ingiuntivo

[42] art. 14 comma 3 del Provvedimento 16 aprile 2014: "*La dimensione massima consentita per la busta telematica è pari a 30 Megabyte.*"

b) Scannerizzazione della procura alle liti autenticata

c) Scannerizzazione della ricevuta di pagamento del contributo unificato (o delle marche da bollo)

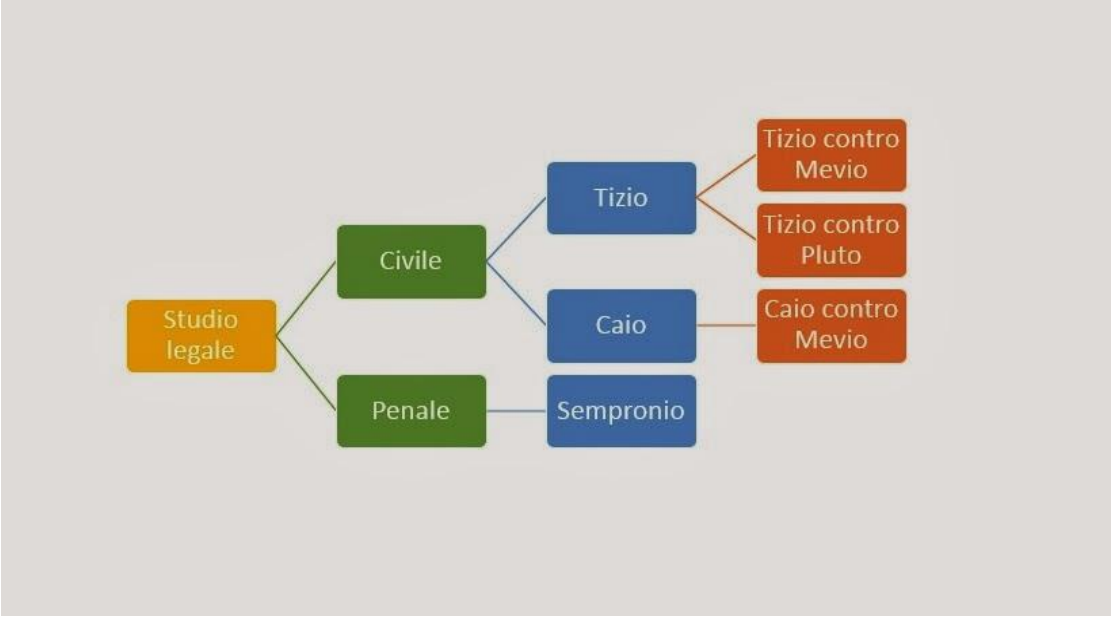
d) Scannerizzazione delle fatture e della ulteriore documentazione

f) Scannerizzazione dell'eventuale estratto autentico delle scritture contabili

Vista la palese proliferazione dei file legati ad un singolo fascicolo, l'Avvocato telematico non potrà più (come invece molti Colleghi continuano imperterriti a fare) salvare i propri atti alla rinfusa nel computer, o semplicemente, dividerli in cartelle per tipologia di atto (es: ricorsi, atti di citazione, appelli etc….).

L'archiviazione dovrà invece seguire uno schema ad albero ramificato, e, ad ogni fascicolo, dovrà corrispondere (come minimo) un'unica cartella.

Lo struttura, ad esempio, potrebbe seguire lo schema che segue:



In questo modo ad ogni fascicolo corrisponderà una sola cartella e, all'interno della cartella, saranno presenti tutti i file relativi a quella pratica.

Sottoparagrafo 2.2.3 – Il Client di posta elettronica

Come sottolineato nel paragrafo precedente la PEC (Posta Elettronica Certificata) è uno degli strumenti indispensabili per il processo civile telematico.

Non solo, infatti, costituisce – già ad oggi – il nostro domicilio informatico a cui vengono recapitati obbligatoriamente tutti i biglietti di cancelleria, ma diventerà il veicolo tramite il quale il nostro atto virtuale arriverà sulla scrivania del cancelliere.

In virtù del massiccio scambio di dati e del notevole numero di ricevute che verranno recapitate al nostro indirizzo PEC, sarà quindi assolutamente indispensabile configurare il client di posta elettronica del nostro studio legale con la posta certificata.

Molti Colleghi hanno l'abitudine di leggere la posta elettronica certificata unicamente tramite applicativi web, limitandosi a controllarla sporadicamente oppure all'arrivo di un messaggio di avviso sulla propria casella mail ordinaria.

A mio avviso una prassi di questo tipo è assolutamente da evitare.

L'utilizzo di un client di posta elettronica, infatti, ci consentirà non solo di automatizzare il download della posta (ad esempio settando l'invio e la ricezione di nuovi messaggi ogni 5 minuti) ma anche di salvare in locale tutte le ricevute dei nostri messaggi di posta certificata.

Ricordo, a tal proposito, che i gestore di PEC hanno l'obbligo di tenere traccia delle operazioni (e delle ricevute) relative ad un determinato indirizzo per 30 mesi, scaduti i quali potrebbero venire – almeno in linea teorica – rimosse dal server.

Proprio per tale ragione (soprattutto in virtù del fatto che la così detta RDAC – ricevuta di avvenuta consegna – della busta telematica attesta il deposito dell'atto e che l'obbligo di conservazione documentale per l'Avvocato è ben più lungo dei 30 mesi *de quo*) è consigliabile salvare una copia locale delle più importanti ricevute di PEC.

Il nostro client di posta farà questa operazione in automatico, salvando in locale tutti i messaggi inviati e ricevuti dal nostro indirizzo di posta elettronica certificata (consiglio in ogni caso di salvare le singole ricevute anche all'interno della cartella del fascicolo di riferimento).

Preciso che può andar bene qualunque client di posta elettronica, dai classici Windows live mail, Outlook express, Windows Mail e Outlook per Windows, a Mail per mac o a Thunderbird per chi – come il sottoscritto – è un accanito sostenitore del software open source.

Sottoparagrafo 2.2.4 – Le password

Con il progressivo aumento della tecnologia e di servizi fruibili attraverso internet, si sono moltiplicate a dismisura le password ed i pin che dobbiamo ricordare.

Comprendo bene che, proprio in virtù del grande numero di password assegnate ad ognuno di noi, molti Colleghi abbiano fatto ricorso a parole chiave piuttosto semplici, quali il nome di un parente o del proprio animale domestico, oppure al proprio codice fiscale.

Questo tipo di prassi, come anche quella di scrivere su foglietti ed agende le password da ricordare, sono assolutamente da evitare, soprattutto per il pin della firma digitale e per la password della PEC.

Per quanto riguarda il pin della firma digitale sarà assolutamente necessario fare uno sforzo di memoria per imparare la serie numerica. Se, infatti, i certificati di firma sono inutilizzabili in caso di furto del supporto (smart card o chiavetta usb), lo stesso non potrà dirsi qualora sulla confezione della chiavetta o sulla smart card abbiate appuntato il pin per non dimenticarlo.

Inutile esemplificare ciò che un malintenzionato potrebbe realizzare tramite uno strumento che consente di sottoscrivere documenti digitali a vostro nome!

Stessa cosa potrà dirsi per la password della PEC.

A tal proposito ricordo a tutti che una password degna di questo nome dovrebbe avere le seguenti caratteristiche minime:

a) Almeno otto caratteri
b) Lettere maiuscole e minuscole
c) Numeri
d) Almeno un simbolo

Per cercare di non perdere traccia delle varie password, quindi, potrebbe essere utile dotarsi di un software atto al così detto *"key store"* che salvi tutte le password che utilizziamo maggiormente e le protegga attraverso una *"master password"* che sarà l'unica da dover tenere a mente.

Tali software sono tranquillamente reperibili in rete e, in alcuni casi, anche con licenze "*free to use"* oppure open source

Sottoparagrafo 2.2.5 – Il backup ed il salvataggio dei dati

Come abbiamo visto nei sottoparagrafi 2.2.1. e 2.2.2. la quantità di dati che i nostri computer immagazzineranno a partire dal prossimo 30 giugno 2014 aumenterà a livello esponenziale.

Un processo di digitalizzazione degno di questo nome, però, non potrà prescindere da adeguati strumenti di archiviazione e conservazione dei dati.

Mi sembra quasi scontato sottolineare che, qualora l'hard disk del nostro pc o del nostro server di studio ci abbandonasse all'improvviso, potremmo dover dire addio ad interi fascicoli e a mesi se non anni di lavoro.

Onde scongiurare un rischio di questo tipo esistono sistemi di back-up e di *storage* dati di diversa tipologia:

A) Il più semplice è certamente il classico hard disk esterno, sul quale l'Avvocato – manualmente o in modo automatico se munito di software specifici – salverà una copia dei dati relativi al proprio studio legale.

Questo sistema, certamente semplice ed intuitivo, presta però il fianco alla fragilità dei supporti di archiviazione che, come ogni altro prodotto elettronico, sono soggetti a guasti più o meno importanti.

B) Allo stesso livello di sicurezza possiamo poi trovare il salvataggio di dati su supporto esterno c.d. "consumabile" (cassette zip, cd, dvd, etc….) a cui possono essere mosse le medesime eccezione di cui al punto precedente, con l'aggiunta di una generale scarsa capacità di archiviazione dei dati se confrontata con quella garantita da un hard disk esterno.

C) Ad un livello di sicurezza superiore si attestano i sistemi di archiviazione basati su server ad hard disk multipli.

Cercando di spiegare in modo semplice il funzionamento di questi sistemi, basti dire che non sono altro che computer centralizzati che immagazzinano tutti i dati della nostra rete e che, invece di salvarli su un unico hard disk presente all'interno del server stesso, li aggiornano in *"mirror"* su almeno due supporti magnetici contemporaneamente, così da garantire – in caso di rottura – l'integrità dei dati sul disco rimanente.

Spesso questi sistemi prevedono anche la possibilità di un salvataggio dati esterno di cui ai precedenti punti A) o B), in modo da scongiurare la possibilità di un crash totale del sistema e – quindi – di tutti i dischi magnetici contemporaneamente.

D) Al maggior livello di sicurezza – almeno ad opinione di chi vi scrive – si attesta poi il c.d. "cloud", ossia un servizio di archiviazione dati esterno che funziona attraverso il web.

Questo sistema permette di caricare sui server dell'azienda che fornisce il servizio (solitamente server altamente tecnologici con cicli di back-up costanti e sistemi di sicurezza all'avanguardia) tutti i dati presenti sul nostro pc di studio, rendendoli – oltretutto – sempre accessibili da qualsiasi supporto connesso alla rete internet.

Unica pecca di un sistema solido e indubbiamente comodo come questo è la possibile vulnerabilità dei dati ad attacchi hacker o a letture esterne, rischio che – benché remoto – non è del tutto eliminabile.

Problematiche relative a diffusione involontaria di dati sensibili e a violazione della normativa della privacy, però, possono essere risolte tenendo presenti le c.d. *best practice*

elaborate dal CCBE (Consiglio degli Ordini Forensi d'Europa) nel settembre del 2012[43], nonché aggiornando la propria informativa sulla privacy.

Oltre a ciò, in virtù dei pericoli sopra evidenziati, è consigliabile utilizzare un servizio di *cloud computing* che operi una crittografazione dei dati al momento dell'archiviazione (come Spideroak oppure Wuala); ciò permetterà di evitare problematiche relative alla privacy ed alla diffusione di dati sensibili anche in caso di attacchi hacker.

A mio avviso, concludendo, uno dei sistemi più duttili e funzionali è certamente rappresentato dal cloud che, oltretutto, ha dei costi di mantenimento esigui se non – in alcuni casi – addirittura nulli.

Molti colossi dell'informatica e della tecnologia, infatti, hanno immesso sul mercato i propri sistemi di cloud, garantendo la gratuità degli stessi fino ad un certo limite di gigabyte di spazio virtuale.

I sistemi più conosciuti sono certamente Onedrive[44], Googledrive[45], Icloud[46], Dropbox[47], SpiderOak[48] e Wuala[49].

Preciso nuovamente che solo gli ultimi due sistemi supportano nativamente la crittografazione dei file – lato server – al momento dell'upload e sono quindi preferibili dal punto di vista della privacy.

---

[43] Per il testo integrale delle linee guida si veda: http://www.consiglionazionaleforense.it/site/home/pubblicazioni/studi-e-ricerche/documento6132.html

[44] https://onedrive.live.com/about/it-it/

[45] http://www.google.com/drive/?usp=ad_search&gclid=CPHM7OSyob0CFYMSwwodL4UA-A

[46] http://www.apple.com/it/icloud/

[47] https://www.dropbox.com/login

[48] https://spideroak.com/

[49] https://www.wuala.com/it/

CAPITOLO 3 – La busta digitale

Chiariti quali siano gli strumenti e le regole di base da adottare in vista del processo civile telematico, non ci resta che occuparci della redazione e dell'invio della busta digitale.

Attività che sostituirà – a partire dal 30 giugno 2014 – il deposito cartaceo degli atti giudiziari visti al Capitolo 1 della presente guida.

L'esposizione che segue cercherà di prescindere dalla tipologia di programma utilizzato per la redazione della busta ma, per gli inevitabili esempi *step by step*, farà riferimento al redattore "SLPCT"[50].

Ciò soprattutto per ragioni, come già detto, di opportunità, posto che – ad oggi e per quanto a conoscenza di chi scrive – è l'unico software open source del settore.

Paragrafo 3.1– La preparazione

Preliminarmente ad ogni altra attività dovremo necessariamente procedere alla preparazione dei file da inserire all'interno della busta telematica.

Detti file varieranno, come anche nel classico deposito in forma cartacea, al variare della tipologia di atto da depositarsi.

In questa sede prenderemo ad esempio il ricorso per decreto ingiuntivo, non tanto perché è stato il primo ad essere introdotto nella sperimentazione sul processo civile telematico, ma in quanto – a mio personale parere – risulta particolarmente adatto ad essere utilizzato per una guida di questa tipologia.

[50] Il programma è scaricabile liberamente dal PDA Regione Toscana https://www.giustizia.toscana.it/cancelleriatelematica o, in alternativa dal *mirror* *http://www.sph3ra.it/redattore-gratuito-slpct/*

Il ricorso per decreto ingiuntivo, infatti, reca con se tutte le problematiche e tutte le difficoltà proprie del deposito di un atto introduttivo del giudizio e, allo stesso tempo, non comporta solitamente problematiche attinenti a termini di scadenza e a ripetibilità del deposito in caso di errore.

Il nostro ricorso per decreto ingiuntivo telematico, quindi, avrà un proprio contenuto minimo in termini di file da allegare, rappresentato da:

1) il ricorso per decreto ingiuntivo vero e proprio;
2) la nota di iscrizione a ruolo;
3) la ricevuta di pagamento del contributo unificato;
4) la procura alle liti;
5) il file datiatto.xml (di cui parleremo compiutamente nel paragrafo seguente).

Parte di questi documenti dovranno essere preparati prima di procedere alla redazione della busta telematica, vediamo quindi come farlo.

Sottoparagrafo 3.1.1 – L'atto principale

In primis dovremo procedere alla preparazione dell'atto da depositarsi. A tal proposito l'art. 12 del già citato "Provvedimento 16 aprile 2014" prescrive che il documento informatico *de quo* debba avere le seguenti caratteristiche:

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 secondo la struttura riportata ai commi seguenti;*

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.*

Tornando quindi al nostro esempio (per ora ci occuperemo dei punti di cui alle lettere a), b) e c) della norma appena citata), il ricorso per decreto ingiuntivo che ci apprestiamo a depositare dovrà innanzitutto essere redatto tramite il programma di elaborazione testi che solitamente utilizziamo (Word, Open Office, Libre Office… etc…) e poi trasformato in un file di tipo PDF attraverso un'operazione di salvataggio (senza restrizioni per le operazioni di copia e stampa) **e non di scannerizzazione**.

Se siete in possesso di un software di redazione testi relativamente recente (successivo al 2007) non avrete problemi a salvare il file direttamene in formato pdf, posto che la maggior parte di detti programmi supportano questa funzionalità nativamente.

Per coloro che hanno a disposizione solo software più datati, come già detto in precedenza, è possibile optare per l'installazione di una stampante virtuale pdf (cioè un applicativo che installa una stampante "non fisica" sul computer e che trasforma il file – simulando una stampa – in un pdf testuale) oppure installare un software di video scrittura più recente.

L’obbligo di utilizzare un pdf testuale per redigere e depositare il nostro atto digitale fa chiaramente emergere la volontà, del legislatore, di permettere alle Cancellerie e al Tribunale di “lavorare” sul file presente nel fascicolo virtuale, ad esempio facendo copia incolla delle nostre conclusioni all’interno della sentenza del Giudice.

Il deposito di un pdf in formato immagine, infatti, non permetterebbe operazioni di questo tipo, poiché le frasi contenute nel file di riferimento non sarebbero riconosciute dal sistema come vero e proprio testo ma come semplice parte di un’immagine.

Sottoparagrafo 3.1.2 – Il contributo unificato

Una volta preparato il nostro atto principale dovremo provvedere al pagamento del contributo unificato ed alla successiva scannerizzazione della ricevuta.

Attualmente le modalità di pagamento del contributo e della marca di iscrizione a ruolo sono 4:

1) Marca da bollo
2) Bollettino postale
3) F23
4) Pagamento telematico (ove abilitato)

Nei primi tre casi avremo bisogno di scannerizzare la ricevuta del pagamento – o la marca da bollo – e poi (questo per prassi consolidata in molti Tribunali) consegnare l’originale della ricevuta al Cancelliere al momento della richiesta delle copie del decreto ingiuntivo emesso.

Copie che, almeno per il momento – in attesa dell’attuazione della normativa di riferimento –, possono essere richieste unicamente in forma cartacea e quindi necessitano dell’accesso “fisico” alla Cancelleria del Tribunale.

Nel caso del pagamento in via telematica, invece, sarà sufficiente allegare la ricevuta digitale alla busta telematica, attraverso il classico procedimento – che vedremo nel paragrafo seguente – di allegazione documenti.

Preciso che non tutti i software attualmente presenti sul mercato supportano quest'ultimo metodo di pagamento e che non tutti i Tribunale sono ancora abilitati alla sua ricezione.

Tramite il portale dei servizi telematici del Ministero della Giustizia[51], è però possibile non solo procedere al pagamento in forma telematica, ma anche verificare quali siano gli Uffici Giudiziari abilitati alla ricezione.

Sottoparagrafo 3.1.3 – La procura alle liti

A questo punto dovremo provvedere alla scannerizzazione della procura alle liti.

La procura potrà essere apposta sia a margine che in calce al nostro ricorso e dovrà essere stata sottoscritta in via analogica dal nostro cliente e da noi autenticata.

Quindi nulla di difforme dalle classiche modalità di rilascio della procura.

Una volta effettuata tale operazione provvederemo a scannerizzare solo la pagina del ricorso contenente la procura e a salvarla su un file pdf contenente, quindi, solo la procura *de quo*.

Detta procedura è specificatamente richiesta dall'art. 83 c.p.c. che, occupandosi della costituzione digitale del difensore, precisa *"Se la procura alle liti è stata conferita su supporto cartaceo, il difensore che si costituisce attraverso strumenti telematici ne trasmette* ***la copia informatica autenticata con firma digitale****…"*.

[51] http://pst.giustizia.it/PST/

Ricordo che, sempre l'art. 83 c.p.c., prevede la possibilità di rilascio della procura alle liti direttamente in formato digitale da parte del cliente, qualora questi sia munito di kit di firma digitale.

In quest'ultimo caso, il cliente provvederà alla sottoscrizione digitale del file "procura alle liti" senza che sia necessaria una successiva autentica da parte del difensore.

Sottoparagrafo 3.1.4 – I documenti

Una volta preparati i 3 file di cui ai sottoparagrafi che precedono potremo passare alla scannerizzazione di tutti i documenti probatori da allegare all'atto.

Raccomando di non scannerizzare tutti i documenti in un unico file ma di realizzare singoli documenti informatici che rechino una denominazione analoga al nostro elenco documenti redatto in coda al ricorso.

Se ad esempio dovessimo redigere un ricorso per decreto ingiuntivo su fattura, potremmo scannerizzare ed allegare:

1) La messa in mora
2) La fattura
3) L'estratto autentico delle scritture contabili

Gli allegati dovranno obbligatoriamente avere uno dei formati specificati all'art. 13 del "Provvedimento 16 aprile 2014":

" a) .pdf;
b) .rtf;
c) .txt;
d) .jpg;
e) .gif;

f) .tiff;

g) .xml.

h) .eml, purché contenenti file nei formati di cui alle lettere precedenti.

i) .msg, purché contenenti file nei formati di cui alle lettere da a ad h.

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."

Come forse alcuni lettori avranno notato, solo con l'emanazione del provvedimento 16 aprile 2014 sono inclusi nell'elenco i formati di file .msg e .eml, ossia, i formati di file in cui vengono solitamente salvate le ricevute dei messaggi di PEC.

Nel precedente provvedimento 18 luglio 2011, infatti, tali tipologie di documenti non erano stati inseriti nell'elenco dei file depositabili con la busta telematica, determinando l'impossibilità per i Colleghi che effettuavano le notificazioni in proprio via PEC (ex art. 3-bis L.53/94) di depositare le ricevute digitali delle proprie notifiche e costringendoli ad un'inutile attività di stampa e ad una successiva attestazione di conformità all'originale.

Il normatore, in questo caso, ha però perso l'opportunità di equiparare realmente Processo Civile e Processo Civile Telematico, poiché con l'introduzione della dicitura: "*h) .eml, purché contenenti file nei formati di cui alle lettere precedenti."* e ancora *"i) .msg, purché*

contenenti file nei formati di cui alle lettere da a ad h.”, ha di fatto sancito l’impossibilità di depositare le classiche mail – non certificate – che non contengano allegati.

Gli scambi di messaggi e le conversazioni che potremmo aver interesse a depositare in Giudizio, quindi, non potranno in realtà trovare posto nel nostro fascicolo digitale, o comunque, se depositate, potrebbero essere oggetto di eccezione da parte del Collega “avversario”.

E’ certamente vero che le classiche mail non certificate, ma anche le PEC, che non contengano in allegato la missiva sottoscritta digitalmente, recheranno informazioni che – secondo prassi e Dottrina – vengono considerate sottoscritte con firma elettronica c.d. semplice e come tali non idonee a fare piena prova in Giudizio ma, unicamente, liberamente valutabili dal Magistrato (si veda il Codice dell’Amministrazione Digitale), ma è allo stesso tempo vero che non può essere il normatore (oltretutto di rango regolamentare) ad impedire ad un Legale di depositare un documento che il Giudice in un procedimento “non telematico” potrebbe comunque – seppur liberamente – valutare.

A questo aggiungo che, quasi sotto silenzio, scompare dall’elenco dei formati di file utilizzabili per gli allegati l’odf (formato di documento aperto)[52].

Eliminazione forse indolore per la maggior parte dei Colleghi ma francamente incomprensibile per chi, come il sottoscritto, da anni promuovere il software libero ed i formati aperti.

[52] http://whatis.techtarget.com/fileformat/ODF-Open-Document-Format

Paragrafo 3.2 – La redazione della busta

Una volta concluse tutte le operazione di redazione e scannerizzazione, ed una volta salvati tutti i documenti su una cartella (magari creata *ad hoc*) sul nostro computer, saremo pronti per passare alla seconda fase della realizzazione della busta telematica.

Come sappiamo, per perfezionare il deposito degli atti *de quo*, dovremo elaborare una busta telematica contenente l'atto principale, tutti gli allegati che normalmente avremmo allegato all'atto cartaceo ed un ulteriore file digitale, denominato Datiatto.xml, che – come suggerisce il nome – conterrà tutti i dati relativi al nostro atto digitale.

La busta dovrà essere preparata attraverso il software di redazione atti scelto dall'Avvocato.

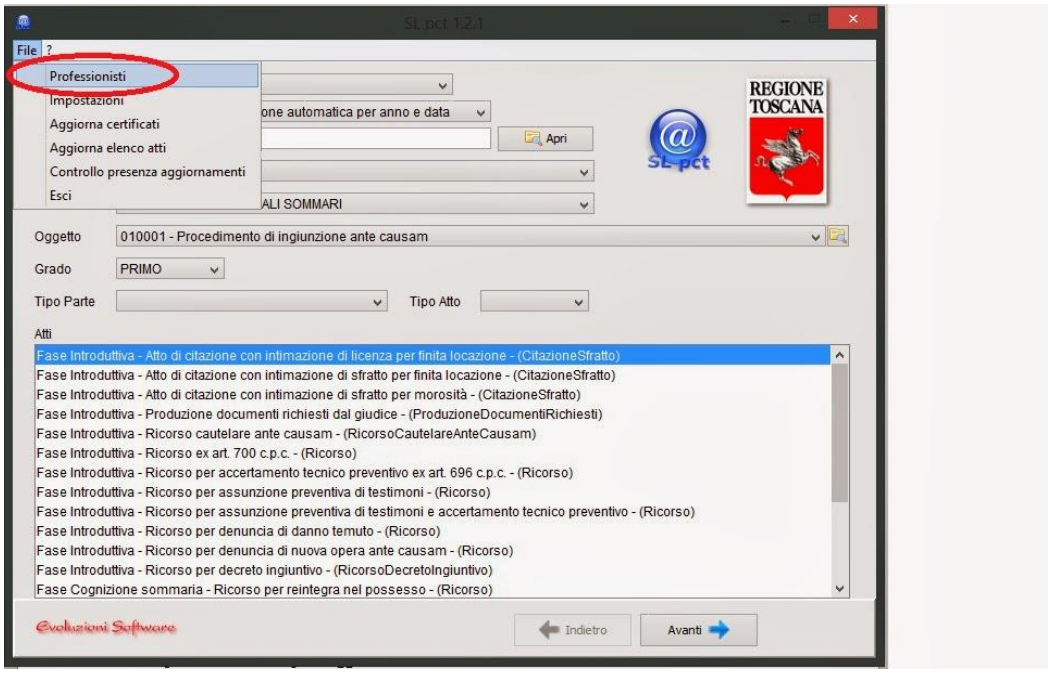
Come già detto nei capitoli precedenti il mio consiglio è di utilizzare il programma SLPCT che rappresenta, ad oggi, l'unica realtà open source in questo ambito professionale.

Pertanto questa fase di preparazione farà riferimento a detto applicativo.

Dopo aver installato il software e, eventualmente, gli altri programmi correlati (SLPCT necessita di Java per funzionare, software scaricabile gratuitamente dalla rete[53]), procederemo al primo avvio del programma.

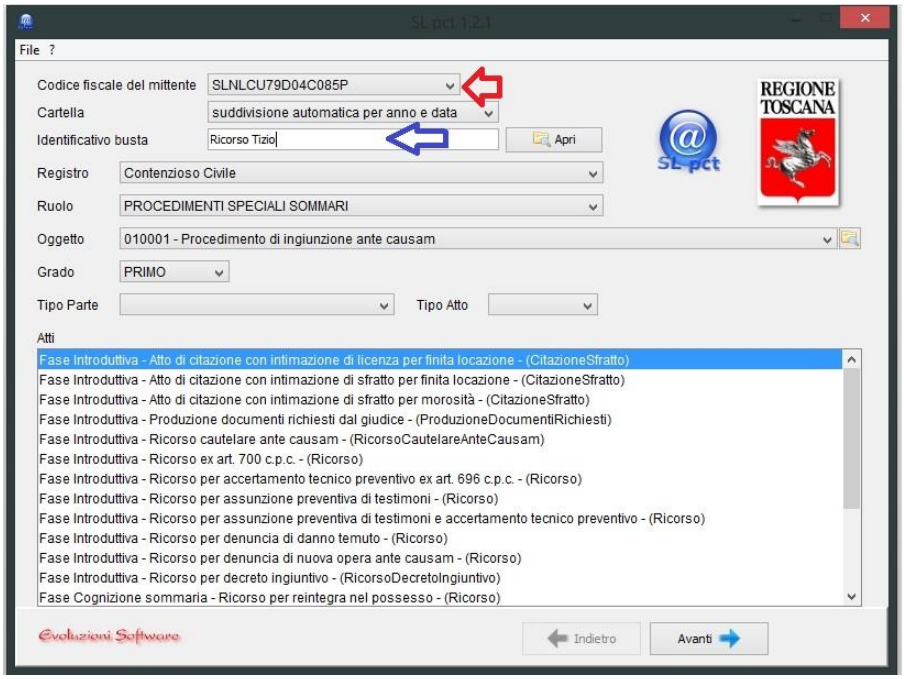
Una volta caricati i certificati degli Uffici Giudiziari (operazione che l'applicativo farà in completo automatismo) dovremo procedere al caricamento della nostra anagrafica, ciò – molto semplicemente – attraverso un click sulla voce "file" presente nella barra grigia in alto (v. fig. 1) e poi su "professionisti".

[53] https://www.java.com/it/download/



(Fig. 1)

Dopo aver inserito tutti i nostri dati (avendo avuto cura di selezionare la casella “mittente di buste per via telematica” nella schermata di caricamento) potremo selezionare il nostro codice fiscale nella prima casella presente in altro (v. fig. 2 freccia rossa)



(Fig 2)

e poi dare un nome alla nostra busta digitale (v. fig 2 freccia blu).

Sottolineo che, per la creazione di una nuova busta, non sarà necessario cliccare sul bottone "apri", che invece servirà nel caso in cui volessimo richiamare un file già precedentemente creato.

Dovremo poi procedere ad inserire tutti i dati del procedimento e, in particolare, tutti quei dati che normalmente avremmo inserito all'interno della nota di iscrizione a ruolo, quali: la Curia, il valore della causa, i dati anagrafici delle parti, etc…..

Tramite l'inserimento da tastiera di questi dati, andremo inconsapevolmente a creare gli ultimi due file "obbligatori" che dovranno far parte del nostro decreto ingiuntivo telematico, ossia, la nota di iscrizione a ruolo (che infatti non era volutamente stata richiamata nella fase di preparazione della busta) e il file "datiatto.xml".

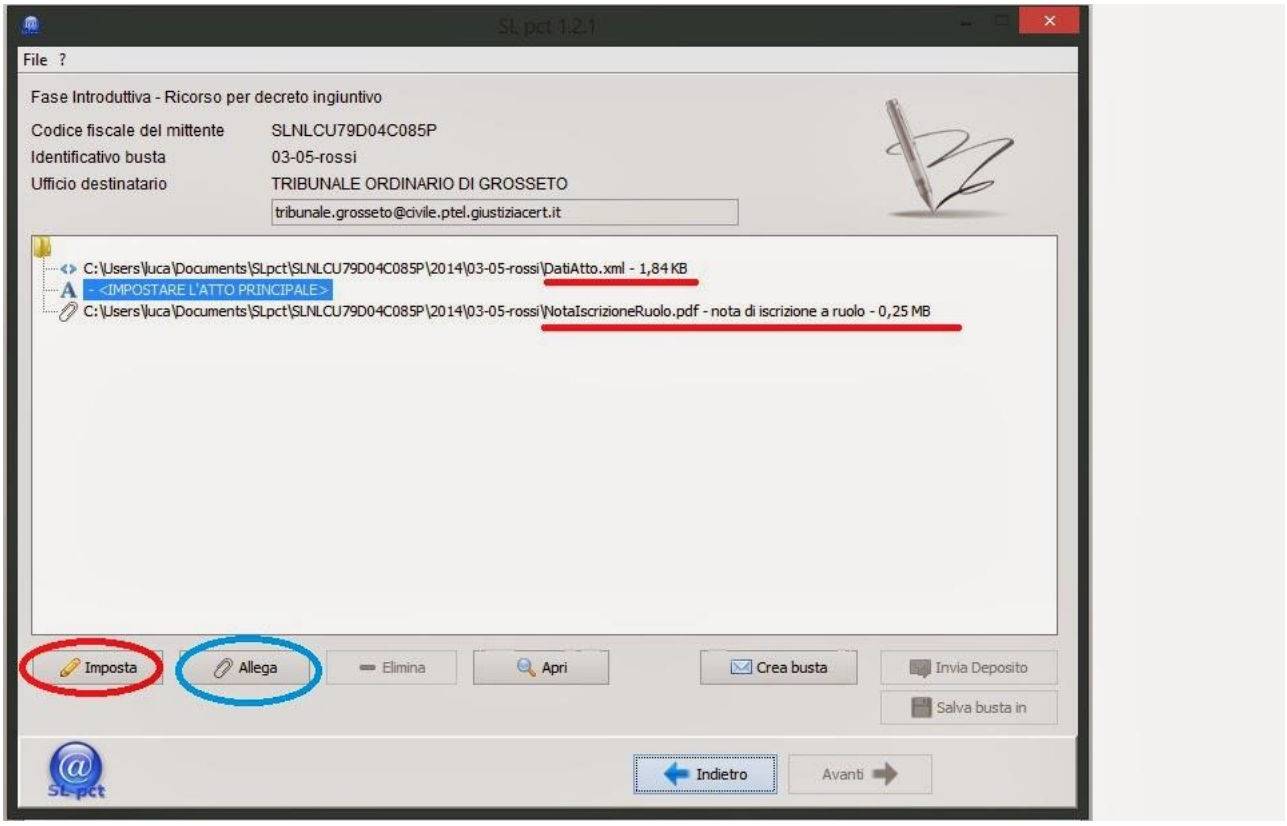
Il file datiatto.xml[54] non è altro che una copia strutturata dei dati già presenti nel nostro ricorso per decreto ingiuntivo, che permetterà al c.d. "sistema giustizia" di acquisire automaticamente i dati del procedimento senza la necessità di un inserimento manuale da parte del Cancelliere.

I dati inseriti in questo file (che devono quindi essere identici a quelli inseriti nell'atto principale) verranno acquisiti in modo automatico dai sistemi informatici ministeriali ed utilizzati per la creazione e per l'aggiornamento del fascicolo.

Alla fine della procedura di inserimento manuale dei dati, ci troveremo di fronte all'elencazione dei file da inserire all'interno della busta telematica.

Posto, quindi, che 2 degli allegati obbligatori sono già presenti nell'elenco dei file da inserire nella busta (v. fig. 3) non ci rimarrà che impostare l'atto principale, cliccando appunto sul bottone imposta (v. fig. 3 cerchio rosso), nonché allegare gli ulteriori file obbligatori, ossia, la ricevuta del pagamento del contributo unificato e la procura alle liti.

[54] Cfr. art 12 lett. e) "Provvedimento 16 aprile 2014"



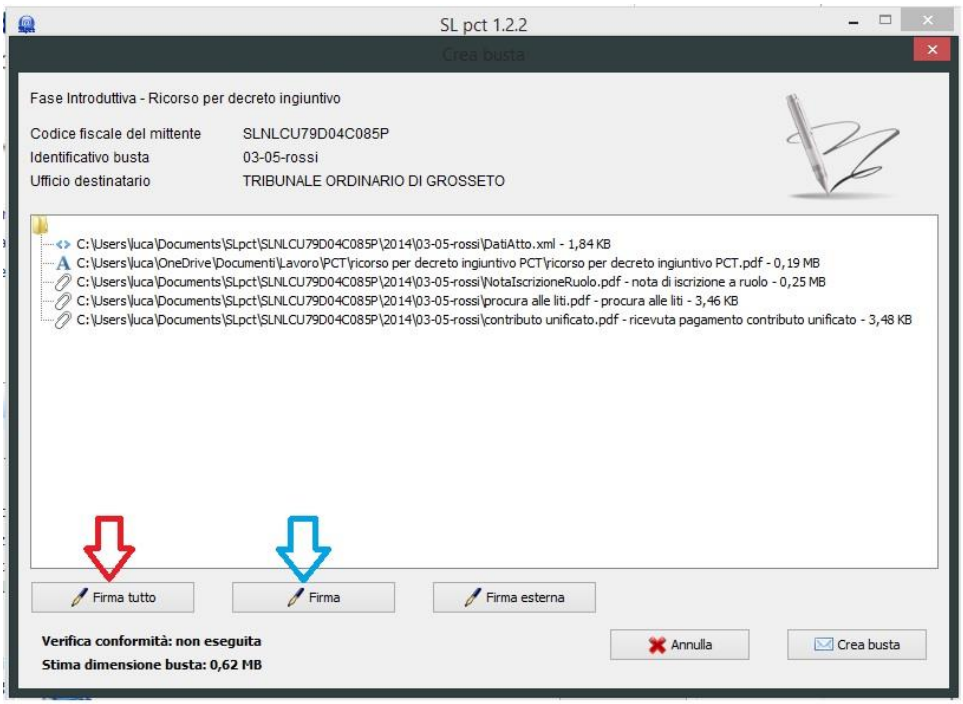
(Fig. 3)

Al caricamento degli allegati, sia obbligatori (o qualificati) che semplici (ossia gli allegati probatori), si procede con un semplice click sul bottone allega (v. fig. 3 cerchio rosso).

Una volta caricati tutti i file necessari all'elaborazione della busta potremo procedere selezionando l'opzione "crea busta", dando quindi il via alla procedura di firma, crittografazione ed invio, che vedremo nella fase successiva.

Paragrafo 3.3 – La firma e l'invio

Dopo aver selezionato l'opzione "crea busta" il programma provvederà ad aprire la finestra deputata alla firma dei documenti caricati (v. fig 4).



(fig.4)

Il software ci darà la possibilità di firmare tutto ciò che abbiamo caricato (cfr. fig. 4 freccia rossa), di firmare singolarmente solo alcuni file (cfr. fig. 4 freccia blu) oppure di utilizzare un software esterno per la sottoscrizione.

Sussiste l'obbligo di sottoscrizione solo di alcuni dei file allegati, ossia – nel caso del ricorso per decreto ingiuntivo –, del file datiatto.xml, dell'atto principale, della procura alle liti scannerizzata e della nota di iscrizione a ruolo.

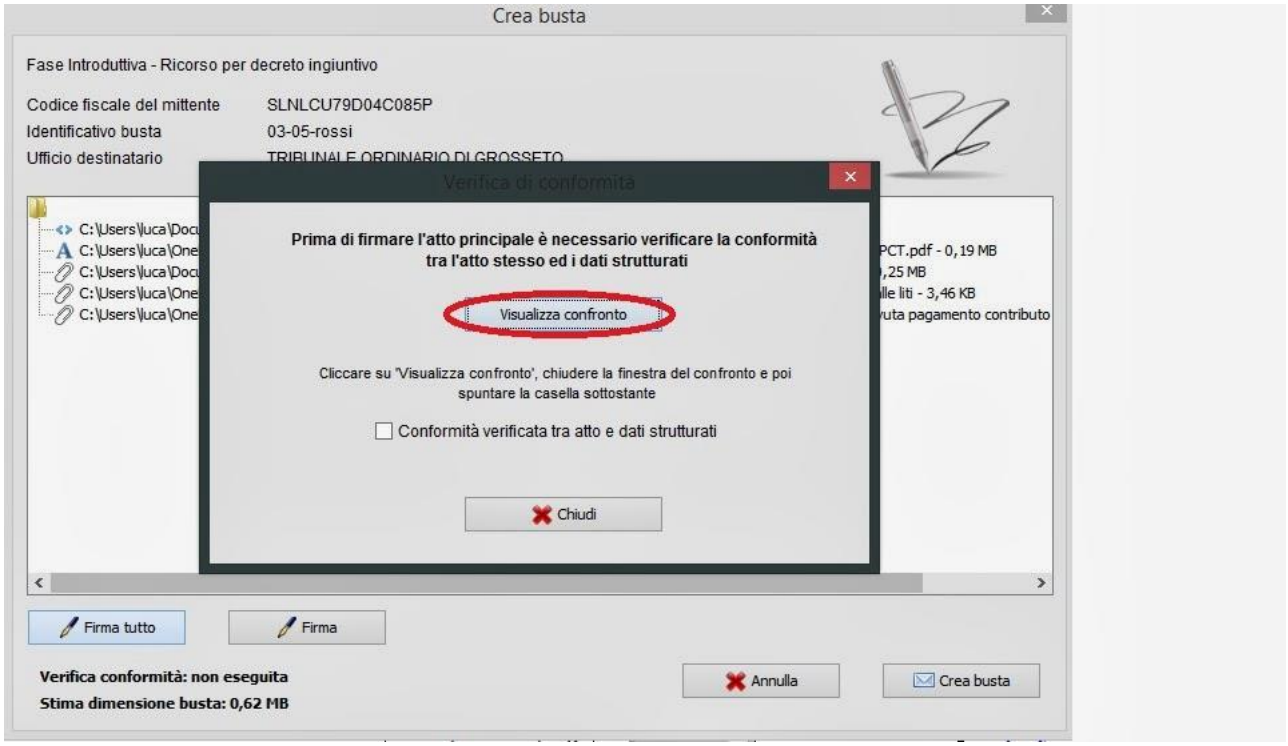
Sostanzialmente, quindi, dovremo obbligatoriamente sottoscrivere tutti i documenti che – di norma – sottoscriveremmo anche in caso di deposito cartaceo, oltre - come detto - al file datiatto.xml.

Nulla vieta, però, di firmare anche gli altri allegati.

Sostanzialmente, quindi, qualora non aveste problemi di spazio (ricordo che la busta telematica può avere una dimensione massima di 30 mb) potrete tranquillamente scegliere l'opzione "firma tutto" (v. fig. 4 freccia rossa).

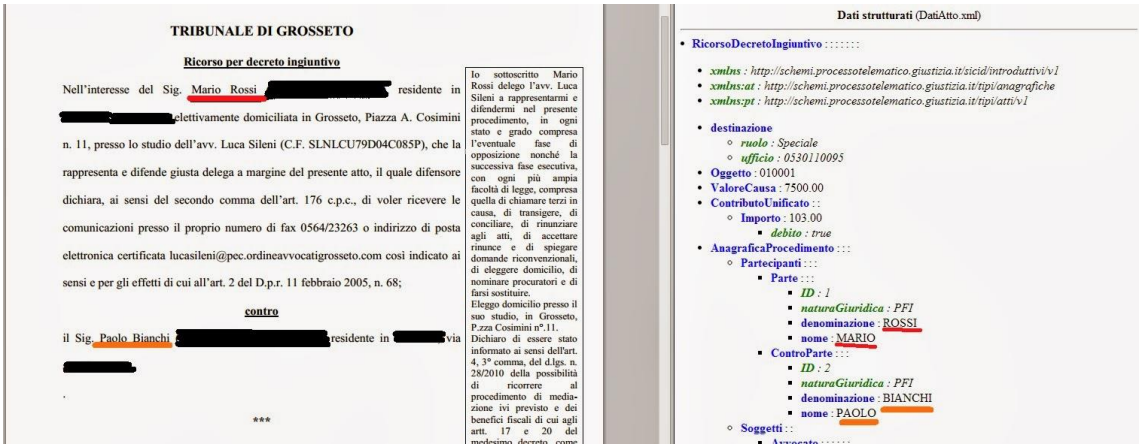
Nel caso, invece, foste vicini a raggiungere il limite di dimensione sopra segnalato (visto che l'operazione di firma aggiunge ulteriore codice informatico al file, facendone crescere il "peso") vi consiglio di sottoscrivere unicamente i file da firmare obbligatoriamente (v. fig. 4 freccia blu).

Ponendo di aver selezionato l'opzione "firma tutto" ci verrà, a questo punto, chiesto di attestare la conformità fra il file "datiatto.xml" ed il nostro ricorso per decreto ingiuntivo. Procediamo, quindi, cliccando su "visualizza confronto" (v. fig. 5).



(fig. 5)

Questa fase, sostanzialmente, rappresenta l'ultimo *step* di controllo permesso dal sistema, passo molto importante perché ci consente di verificare, mettendo a confronto i dati caricati nel file xml (sulla destra - v. fig. 6) e quelli presenti nel nostro atto (sulla sinistra - v. fig. 6), di non aver commesso errori nella redazione della busta.

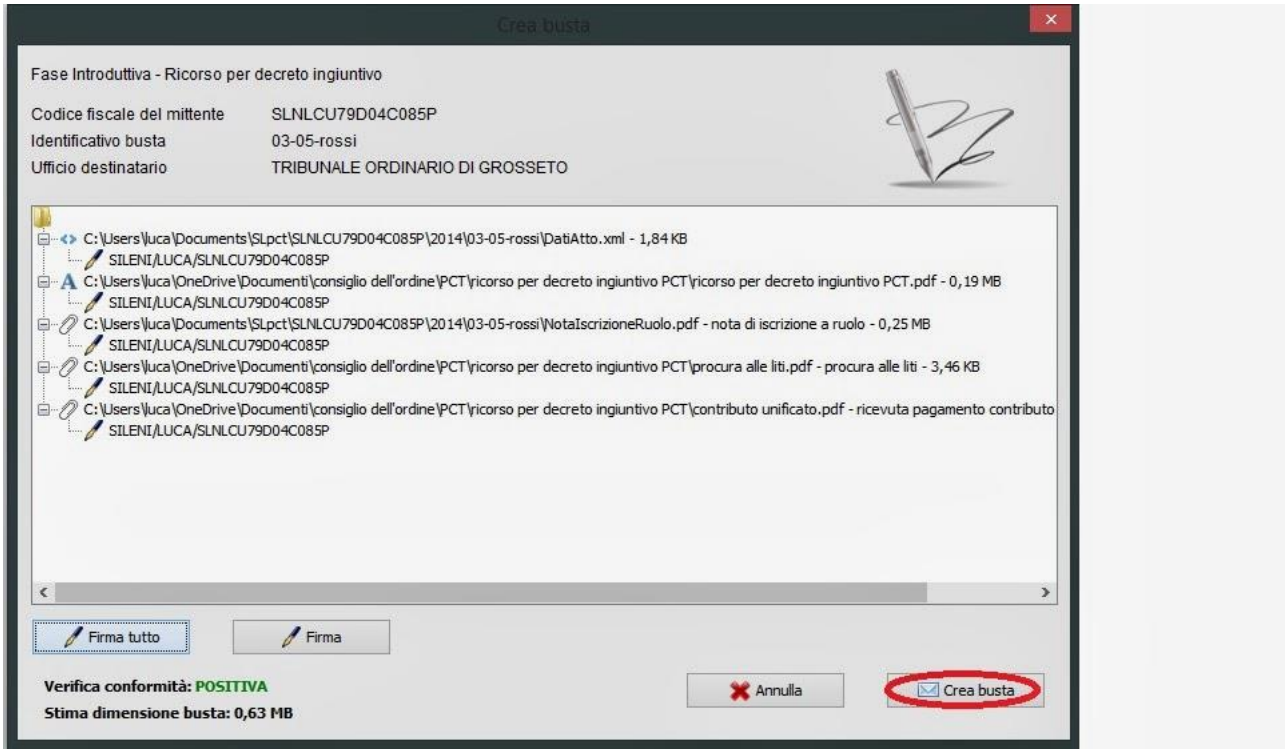


(fig. 6)

Vi raccomando la massima attenzione nell'analisi del confronto video, poiché i due file (l'atto in formato pdf ed il datiatto.xml) dovranno necessariamente essere reciprocamente conformi nel contenuto.

Qualora vi sia corrispondenza fra i dati inseriti nei due file non dovremo far altro che chiudere la finestra di confronto, collegare il nostro kit di firma digitale al computer, spuntare la casella "conformità verificata" (v. fig. 5) e poi inserire il PIN.

Una volta firmati i file dovremo cliccare nuovamente su "crea busta" (v. fig. 7), avviando così il processo di crittografazione del documento informatico da inviare alla cancelleria del Tribunale.

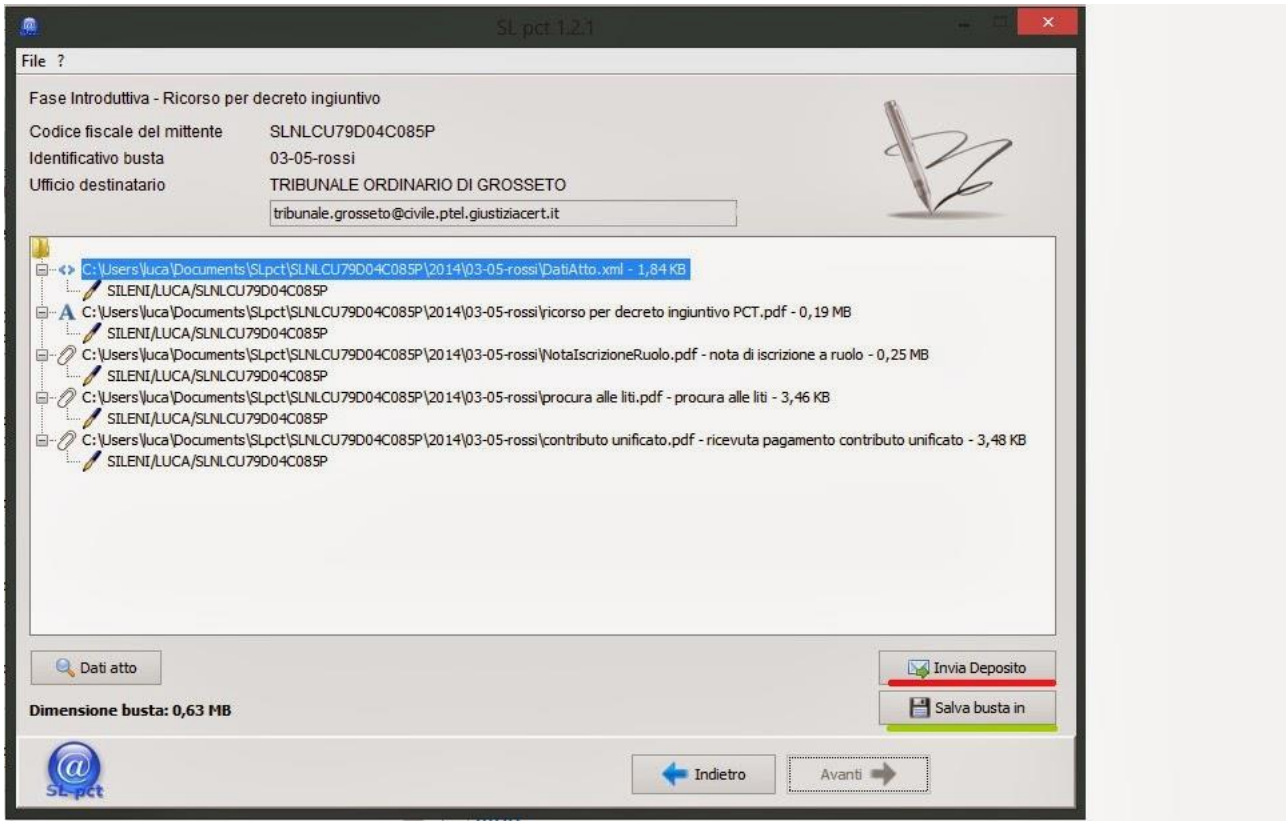


(fig. 7)

Conclusa la fase di crittografazione, il programma restituirà il file “Atto.enc” che altro non è se non la nostra busta telematica.

A questo punto il software ci permetterà di salvare la busta sul computer (ad esempio per inviarla tramite un client webmail, o attraverso un PDA) o anche di inviarla direttamente (scelta che vi consiglio caldamente) attraverso il vostro client e-mail predefinito.

In quest’ultimo caso non dovremo far altro che cliccare sul bottone “invia deposito” (v. fig. 8 – sottolineatura in rosso)



(fig. 8)

ed il programma provvederà a creare automaticamente un nuovo messaggio attraverso il vostro client di posta elettronica, che recherà già – quale allegato – il file "atto.enc", nonché le giuste indicazioni del destinatario e dell'oggetto del messaggio, che vi raccomando di non modificare.

Non dovrete quindi far altro che selezionare il mittente (ossia il vostro indirizzo PEC che avrete già configurato con il client di posta elettronica) e premere invio, lasciando in bianco il corpo della mail.

Una volta premuto il tasto invio, il flusso dei dati previsti dalla normativa tecnica è, sostanzialmente, il seguente:

1) il messaggio PEC viene inviato e ricevuto dal gestore di posta elettronica certificata del Legale depositante;

2) il gestore di PEC del depositante genera ed invia al mittente la RDA (Ricevuta Di Accettazione) – questo vi permetterà di sapere che il vostro messaggio è stato correttamente inoltrato ed è in attesa di consegna al destinatario;
3) il messaggio di posta elettronica viene poi inviato al gestore PEC del Ministero della Giustizia (denominato GiustiziaCert);
4) GiustiziaCert genera ed invia al depositante la RDAC (Ricevuta Di Avvenuta Consegna) che attesta il momento della ricezione, da parte dei server ministeriale, della busta telematica – è importante ricordare che indipendentemente dalle successive operazioni di controllo, la data e l'ora di deposito del fascicolo virtuale saranno quelle indicate nella RDAC;
5) il gestore dei servizi telematici del Ministero, poi, provvederà a scaricare il nostro messaggio di posta elettronica certificata e ad effettuare una serie di controlli formali sulla busta telematica, quali:
    a) Verifica delle dimensioni della busta
    b) Verifica che il mittente sia censito nel RegIndE
    c) Verifica del formato del file allegato alla busta
6) il gestore dei servizi telematici del Ministero provvederà poi ad inviarci l'esito dei controlli formali effettuati e, in caso di esito positivo, renderà disponibile la busta per l'apertura da parte dell'operatore di Cancelleria;
7) in orario di ufficio, e quindi probabilmente la mattina successiva al nostro inoltro via PEC, il Cancelliere provvederà a scompattare la busta telematica e a verificarne il contenuto provvedendo, in caso di assenza di errori o anomalie, a depositare l'atto e gli allegati nel fascicolo informatico;

8) il gestore dei servizi telematici del Ministero, all'esito dei controlli del personale di Cancelleria, invierà l'ultimo messaggio di PEC al depositane, dando atto dell'avvenuto positivo deposito dell'atto o, in alternativa, dell'errore riscontrato dal Cancelliere.

Da un'analisi, anche sommaria, del flusso dei dati informatici necessario al deposito di un qualsiasi atto digitale, salta subito agli occhi come l'attività del Cancelliere – che accetta l'atto e fa partire l'ultima ricevuta di conferma – resti comunque centrale ed assolutamente ineliminabile.

Nonostante, infatti, la data del deposito sia fatta risalire al momento della generazione della RDAC, l'eventuale rifiuto della busta (per errori di vario genere) da parte del cancelliere, comporterà comunque la necessità di inviare un nuovo atto correttamente redatto, con il rischio che *medio tempore* sia scaduto il termine per il deposito.[55]

E' chiaro altresì che, nonostante sia virtualmente possibile depositare a qualunque ora del giorno e della notte, la Cancelleria di riferimento continuerà ad avere i canonici orari di ufficio e, per tale ragione, sarà consigliabile depositare almeno la sera prima del giorno di scadenza per il deposito, se non addirittura con uno o due giorni di anticipo, onde avere la possibilità – in caso di errori bloccanti – di effettuare tempestivamente un nuovo invio.

[55] Sul punto si veda la recente ordinanza del Tribunale di Perugia commentata al sottoparagrafo 4.3.2

CAPITOLO 4 – Prassi e giurisprudenza

Conclusa l'analisi degli elementi essenziali del processo civile telematico è però – a questo punto – necessario addentrarci nello studio di alcune problematiche applicative che, negli anni di sperimentazione del PCT, hanno già dato origine ad alcune pronunce giurisprudenziali.

Paragrafo 4.1. Il domicilio digitale dell'Avvocato.

Con l'avvento della digitalizzazione del processo civile si è assistito – già a partire dal 2005 con l'introduzione del Codice dell'Amministrazione Digitale – ad un progressivo ricorso allo strumento della Posta Elettronica Certificata. Strumento che, come già sottolineato nei capitoli precedenti, rappresenta un'innovazione tutta italiana, volta ad adeguare le necessità di certezza di ricezione e di invio delle comunicazioni giudiziarie alla classica posta elettronica.

Negli ultimi anni, quindi, si assistito alla progressiva nascita di quello che può essere chiamato "domicilio digitale".

Tale area "virtuale" di ricezione delle comunicazioni, rappresenta - per quanto attinente alla nostra professione - una sorta di surrogato o se vogliamo di "clone digitale" del nostro indirizzo fisico di studio.

L'art. 125 c.p.c. – come novellato dalla L. 183/2011 e dal successivo D.L. 138/2011[56] – prescrive l'obbligo, per ogni Difensore, di *"indicare l'indirizzo di posta elettronica certificata comunicato al proprio ordine"*, sancendo quindi la nascita di un vero e proprio

[56] art. 125 comma I c.p.c *"Salvo che la legge disponga altrimenti, la citazione, il ricorso, la comparsa, il controricorso, il precetto debbono indicare l'ufficio giudiziario, le parti, l'oggetto, le ragioni della domanda e le conclusioni o l'istanza, e, tanto nell'originale quanto nelle copie da notificare, debbono essere sottoscritti dalla parte, se essa sta in giudizio personalmente, oppure dal difensore che indica il proprio codice fiscale. Il difensore deve, altresì, indicare l'indirizzo di posta elettronica certificata comunicato al proprio ordine e il proprio numero di fax"*

domicilio virtuale presso il quale verranno effettuate le comunicazione al Difensore costituito.

Tale norma, che richiama l'indirizzo PEC comunicato all'Ordine degli Avvocati di riferimento, si armonizza perfettamente con l'art. 16 del D.M. 44/2011 (provvedimento cardine del processo civile telematico), il quale prevede l'obbligatorietà, per le cancellerie, di effettuare le comunicazioni indirizzate all'Avvocato costituito in giudizio all'indirizzo PEC risultante dal RegIndE[57].

Come sappiamo il RegIndE viene "alimentato" anche grazie all'invio periodico, da parte di tutti gli Ordini degli Avvocati, degli indirizzi di Posta Elettronica Certificata di ciascun iscritto. In tal modo si cerca di raggiungere una sorta di identità "teorica" fra l'indirizzo PEC che deve essere comunicato ex art. 125 c.p.c. e quello prescritto per le comunicazioni ex art. 16 D.M. 44/2011.

Se tutte le comunicazioni di cancelleria debbono quindi essere indirizzate alla PEC del Difensore costituito, e se quindi tale indirizzo di posta elettronica certificata (anche in ossequio agli artt. 125 e 366 c.p.c.) rappresenta un vero e proprio domicilio virtuale dell'Avvocato, come potrà amalgamarsi tale innovazione normativa con il disposto dell'art. 82 R.D. n 37 del 1934 ? [58]

---

[57] art. 16 comma I del D.M. 44/2011 *"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."*

[58]art. 82 R.D. n 37 del 1934 *"I procuratori, i quali esercitano il proprio ufficio in un giudizio che si svolge fuori della circoscrizione del Tribunale al quale sono assegnati, devono, all'atto della costituzione nel giudizio stesso, eleggere domicilio nel luogo dove ha sede l'autorità giudiziaria presso la quale il giudizio è in corso. In mancanza della elezione di domicilio, questo si intende eletto presso la cancelleria della stessa autorità giudiziaria."*

L'articolo testé richiamato, come tutti i Colleghi sanno, prevede l'obbligatorietà, per tutti gli Avvocati che esercitino il loro Ufficio al di fuori della circoscrizione del Tribunale alla quale sono assegnati, di eleggere domicilio nella circoscrizione ove ha sede l'Autorità Giudiziaria adita.

In virtù di detta disposizione normativa, quindi, l'Avvocato telematico, pur in possesso di una PEC funzionante e quindi di un vero e proprio domicilio virtuale, sarebbe ipoteticamente costretto ad eleggere domicilio presso un Collega al fine di svolgere il proprio Ufficio al di fuori della circoscrizione del Tribunale di assegnazione.

A risolvere il contrasto fra le novità normative del 2011 e l'ancora vigente art. 82 R.D. 37/34 sono state però le Sezioni Unite della Corte di Cassazione che, occupandosi di dirimere un contrasto giurisprudenziale di differente origine, hanno avuto modo di occuparsi anche delle riforme finalizzate alla digitalizzazione dei procedimento giudiziari.

Con la sentenza 10143/2012 le SS.UU. della Corte di Cassazione[59] [60] hanno espresso il seguente principio di diritto: "*Il R.D. n. 37 del 1934, art. 82 che prevede che gli avvocati, i quali esercitano il proprio ufficio in un giudizio che si svolge fuori della circoscrizione del tribunale al quale sono assegnati, devono, all'atto della costituzione nel giudizio stesso, eleggere domicilio nel luogo dove ha sede l'autorità giudiziaria presso la quale il giudizio è in corso, e che in mancanza della elezione di domicilio, questo si intende eletto presso la cancelleria della stessa autorità giudiziaria - trova applicazione in ogni caso di esercizio dell'attività forense fuori dalla circoscrizione cui l'avvocato è assegnato per*

[59] La sentenza è reperibile in internet all'indirizzo http://www.ordavvsa.it/images/articoli/files/1328.pdf

[60] Pronuncia recentemente ribadita dalla sentenza 28 novembre 2013, n. 26696 della sez. VI-2 della Corte di Cassazione**.** Per approfondimenti si rimanda a questo articolo del Collega Michele Iaselli: http://www.altalex.com/index.php?idnot=66611

essere iscritto al relativo ordine professionale del circondario e quindi anche nel caso in cui il giudizio sia in corso innanzi alla corte d'appello e l'avvocato risulti essere iscritto ad un ordine professionale di un tribunale diverso da quello nella cui circoscrizione ricade la sede della corte d'appello, ancorché appartenente allo stesso distretto della medesima corte d'appello. Tuttavia, dopo l'entrata in vigore delle modifiche degli artt. 366 e 125 c.p.c., apportate rispettivamente dalla L. 12 novembre 2011, n. 183, art. 25, comma 1, lett. i), n. 1), e dallo stesso art. 25, comma 1, lett. a), quest'ultimo modificativo a sua volta del D.L. 13 agosto 2011, n. 138, art. 2, comma 35-ter, lett. a), conv. in L. 14 settembre 2011, n. 148, e nel mutato contesto normativo che prevede ora in generale l'obbligo per il difensore di indicare, negli atti di parte, l'indirizzo di posta elettronica certificata comunicato al proprio ordine, si ha che dalla mancata osservanza dell'onere di elezione di domicilio di cui all'art. 82 per gli avvocati che esercitano il proprio ufficio in un giudizio che si svolge fuori della circoscrizione del tribunale al quale sono assegnati consegue la domiciliazione ex lege presso la cancelleria dell'autorità giudiziaria innanzi alla quale è in corso il giudizio solo se il difensore, non adempiendo all'obbligo prescritto dall'art. 125 c.p.c., non abbia indicato l'indirizzo di posta elettronica certificata comunicato al proprio ordine".

Come appare assolutamente lampante, il principio espresso dalla Suprema Corte a Sezioni Unite rappresenta una vera e proprio rivoluzione copernicana in materia di domiciliazione.

Cessa ogni obbligo per il Difensore di domiciliarsi presso un Collega con studio nella circoscrizione del Tribunale adito e, allo stesso tempo, viene incontrovertibilmente confermata l'effettiva nascita del così detto "domicilio virtuale" dell'Avvocato, ossia, di

un domicilio non più fisico e ben delimitato a livello spaziale, ma incorporeo e senza una precisa collocazione geografica.

La Suprema Corte, in fin dei conti, nulla ha fatto se non attualizzare l'idea economicistica per la quale vide la luce l'attuale formulazione dell'art. 82 R.D. 37/34, ossia, rendere più agevoli le comunicazioni verso i Difensori costituiti in giudizio.

Gli Ermellini, in effetti, hanno compreso appieno l'estrema flessibilità della PEC e l'innegabile semplicità che si lega inscindibilmente al suo utilizzo.

Utilizzare un account di posta elettronica, materialmente, rende del tutto nulle le distanze spaziali fra due soggetti, distanze che – invece – permangono (e sono spesso di ostacolo) nelle comunicazioni analogiche che viaggino per posta ordinaria.

Sancito, quindi, il venir meno – senza une vera e propria abrogazione della norma di cui all'art. 82 R.D. 37/34 – dell'obbligatorietà di domiciliazione per l'Avvocato telematico, sono però già emersi dubbi e problematiche interpretative legate al domicilio virtuale.

Recentemente, in particolare, mi sono confrontato con alcuni Colleghi su uno specifico caso di studio che – probabilmente – alcuni dei lettori di questa guida avranno già avuto modo di incrociare lungo il loro cammino professionale:

"Qualora un Avvocato con studio – ad esempio – in Roma, avesse richiesto un decreto ingiuntivo a Milano senza domiciliarsi presso un Collega, ma indicando unicamente il proprio indirizzo di Posta Elettronica Certificata ed il proprio indirizzo di studio in Roma, come potrebbe l'ipotetico difensore dell'intimato notificare l'atto di citazione in opposizione a decreto ingiuntivo?"

Teoricamente ben potrebbe notificarlo alla PEC del Collega romano, ma qualora il Difensore di parte opponente non fosse abilitato alle notificazioni in proprio[61], come potrebbe perfezionare la notificazione dell'opposizione?

Una risposta data dalla legge – almeno in linea di principio – esiste, ossia, effettuare la notificazione via PEC avvalendosi del servizio UNEP ex art. 17 D.M. 44/2011 [62]; solo che, come la maggior parte dei Colleghi già sa, i nostri Ufficiali Giudiziari non sono ancora attrezzati per le notificazioni via posta elettronica certificata e non posso quindi dare seguito ad eventuali istanze di questo tipo.

A questo punto, stante il disposto dell'art. 82 R.D. 37/34 e vista l'impossibilità di provvedere alla notificazione via PEC, il nostro ipotetico Collega milanese potrebbe essere orientato ad effettuare la notificazione in Cancelleria applicando pedissequamente l'articolo *de quo* ma contravvenendo, di fatto, al principio di diritto espresso dalla sentenza n° 10143/2012 delle SS.UU., che giudica superata, in presenza dell'indicazione

[61] Ex art. 3-bis L. 53/94

[62] Art. 17 D.M. 44/2011: *Al di fuori dei casi previsti dall'articolo 51, del decreto-legge 25 giugno 2008, n. 112, convertito con modificazioni dalla legge 6 agosto 2008, n. 133, e successive modificazioni, le richieste telematiche di un'attività di notificazione da parte di un ufficio giudiziario sono inoltrate al sistema informatico dell'UNEP, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.*
2. Le richieste di altri soggetti sono inoltrate all'UNEP tramite posta elettronica certificata, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
3. La notificazione per via telematica da parte dell'UNEP rispetta i requisiti richiesti per la comunicazione da un ufficio giudiziario verso i soggetti abilitati esterni di cui all'articolo 16.
4. Il sistema informatico dell'UNEP individua l'indirizzo di posta elettronica del destinatario dal registro generale degli indirizzi elettronici, dal registro delle imprese o dagli albi o elenchi costituiti ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008, n. 185 convertito con modificazioni dalla legge 28 gennaio 2009, n. 2, nonché per il cittadino dall'elenco reso consultabile ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 in base alle specifiche tecniche stabilite ai sensi dell'articolo 34.
5. Il sistema informatico dell'UNEP, eseguita la notificazione, trasmette per via telematica a chi ha richiesto il servizio il documento informatico con la relazione di notificazione sottoscritta mediante firma digitale e congiunta all'atto cui si riferisce, nonché le ricevute di posta elettronica certificata, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.
6. L'ufficiale giudiziario, se non procede alla notificazione per via telematica, effettua la copia cartacea del documento informatico, attestandone la conformità all'originale, e provvede a notificare la copia stessa con le modalità previste dalla normativa processuale vigente.

– ex artt. 125 e 366 c.p.c. – dell'indirizzo di PEC comunicato al proprio Ordine degli Avvocati, la necessità di una domiciliazione fisica da parte del Difensore.

A mio personale avviso, anche in ossequio alla prassi di alcuni Tribunali sul punto, il Difensore di parte opponente dovrà invece attivarsi per provvedere ad una notificazione analogica (cartacea) all'indirizzo romano dell'Avvocato che ha dato avvio al procedimento monitorio.

Il tema rimane in ogni caso aperto ed auspico che tali problematiche vengano presto superate dall'avvio dei servizi di notificazione digitali da parte degli uffici UNEP.

Paragrafo 4.2 Il superamento del limite dei 30 mb

Come ho avuto modo di segnalare nei capitoli precedenti, la busta telematica allegata al messaggio di posta elettronica certificata non potrà avere una dimensione superiore a 30 mb, così come prescritto dall'art. 14 comma 3 del "Provvedimento 16 aprile 2014"[63].

La previsione di un limite nel "peso" della busta telematica non è stata però accompagnata da una normativa che consentisse di aggirare il problema di una produzione abbondante di documenti informatici all'interno del fascicolo digitale.

Nel nostro ordinamento, infatti, non è ad oggi prevista alcuna soluzione normativa al problema segnalato.

In virtù, quindi, delle problematiche applicative che detto limite ha portato con se, le commissioni miste (Magistrati-Avvocati-Cancellieri) attive presso i Tribunali ove la sperimentazione sul PCT è iniziata già da qualche anno, sono intervenute direttamente sulla questione colmando il chiaro vuoto normativo con la produzione di prassi operative.

[63] dall'art. 14 comma 3 del Provvedimento 16 aprile 2014: "*La dimensione massima consentita per la busta telematica è pari a 30 Megabyte."*

Nel caso del ricorso per decreto ingiuntivo, ad esempio, sia le prassi del Tribunale di Firenze[64], che quelle di altri Fori prevedono la redazione di una busta che rechi solo una parte dei documenti probatori da allegare, ma - allo stesso tempo - l'elenco integrale dei documenti prodotti.

Una volta effettuato il deposito si provvederà ad avvertire il Cancelliere che si è depositato una busta incompleta, così che egli possa far emettere al Magistrato assegnatario del procedimento una richiesta di integrazione documentale ex art. 640 c.p.c.

Nel caso di specie, in effetti, le prassi operative non hanno supplito direttamente al problema del limite dimensionale della busta telematica, posto che il nostro codice di procedura civile prevede già uno strumento atto ad integrare l'eventuale carenza di produzione documentale, ossia, il sopracitato art. 640 c.p.c.[65].

L'Avvocato telematico che debba depositare un ricorso per decreto ingiuntivo *"oversize"*, quindi, dovrà semplicemente seguire la procedura di cui sopra, provvedendo a depositare una successiva busta integrativa contenente la documentazione mancante.

Diverso, invece, è il problema dell'eventuale eccessiva dimensione della busta nel caso di memoria 183 c.p.c.

Ad oggi il problema non è ancora stato affrontato approfonditamente dai nostri Tribunali e dovrà essere risolto, se non attraverso prassi interpretative, tramite un auspicabile intervento normativo chiarificatore.

Si precisa che, in effetti, fra le tipologie di buste telematiche depositabili in giudizio, vi è anche una fantomatica "Integrazione documentale richiesta dal Giudice" che sembrerebbe rendere applicabile la prassi di cui al punto precedente anche agli atti giudiziari diversi dal ricorso per decreto ingiuntivo.

---

[64] Art. 29 Protocollo PCT dell'Osservatorio sulla Giustizia Civile di Firenze http://www.osservatoriogiustiziacivilefirenze.it/public/OGCALL_163_0_1.pdf

[65] Art. 640 c.p.c. *"Il giudice, se ritiene insufficientemente giustificata la domanda, dispone che il cancelliere ne dia notizia al ricorrente, invitandolo a provvedere alla prova.*
Se il ricorrente non risponde all'invito o non ritira il ricorso oppure se la domanda non è accoglibile, il giudice la rigetta con decreto motivato.
Tale decreto non pregiudica la riproposizione della domanda, anche in via ordinaria."

Sostanzialmente, quindi, la procedura potrebbe essere analoga a quella sopra citata, con l'unica differenza che, a seguito della comunicazione di "carenza documentale" fatta dall'Avvocato all'indirizzo del Cancelliere e da quest'ultimo al Giudice, il Magistrato non richiederà un'integrazione ex art. 640 c.p.c. ma emetterà un provvedimento generico per autorizzare l'ulteriore produzione di documenti.

Come detto, posto che il problema è ben conosciuto da tutti i pratici del Processo Civile Telematico – e lo è da molti anni –, auspico un rapido e chiaro intervento legislativo ben prima del temine del 30 giugno 2014.

Paragrafo 4.3 – Il "tempo" del deposito telematico

Fra i vari argomenti di discussione che la sperimentazione sul PCT ha generato negli ultimi anni, uno dei più attuali è certamente il "tempo" del deposito.

Proprio negli ultimi mesi, infatti, sono intervenuti due interessanti provvedimenti giudiziari, il primo sul limite delle ore 14.00 per l'invio della busta telematica e il secondo in materia di rimessione in termini.

Sottoparagrafo 4.3.1 – Il limite delle ore 14.00

In ordine alla prima questione, il Tribunale di Milano, con la Sentenza n. 3115 del 3 marzo 2014[66], ha ritenuto di dover risolvere un presunto contrasto fra la norma di cui all'articolo

[66] Il testo completo del provvedimento è stato recentemente pubblicato sul sito Altalex http://www.altalex.com/index.php?idnot=66734

13, comma 2 e 3, D.M. 44/2011[67] ed il disposto dell'articolo 16 bis, comma 7, D.L. 179/2012[68].

Il primo provvedimento normativo – come abbiamo visto nei capitoli precedenti – sancisce l'obbligo di provvedere alla trasmissione della busta telematica entro le 14.00 del giorno di scadenza per il deposito, mentre il comma 7 del D.L. 179/2012 non fa riferimento ad orari particolari per il deposito dell'atto telematico, limitandosi a stabilire che il "*deposito di cui ai commi da 1 a 4 si ha per avvenuto al momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del ministero della giustizia."*

Trovandosi dinanzi ad un presunto contrasto fra norme di rango decisamente diverso, il Tribunale di Milano ha risolto la questione ritenendo *"che la norma di legge di cui all'art. 16bis comma 7 debba ritenersi in ogni caso prevalente rispetto alla norma tecnica regolamentare perché è una fonte primaria rispetto a quella tecnica che ha natura secondaria, è in ogni caso temporalmente successiva a quella regolamentare che prevede un limite temporale non autorizzato né previsto da una fonte primaria ed in contrasto con la norma codicistica di carattere generale sopra richiamata che in nessun caso può ritenersi possa essere superata in forza di una norma avente rango inferiore."*

Ad avviso del Giudice Milanese, quindi, a nulla rileverebbe l'indicazione delle ore 14.00 per il deposito della busta telematica, potendosi invece ritenere tempestivamente

---

[67] *"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."

[68] *7. Il deposito di cui ai commi da 1 a 4 si ha per avvenuto al momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del ministero della giustizia.*

depositata la memoria digitale la cui RDAC (ricevuta di avvenuta consegna) sia generata entro le ore 23.59 del giorno di deposito (nel caso di specie la generazione era avvenuta alle ore 14.27 e quindi 27 minuti dopo la scadenza dell'orario previsto dal D.M. 44/2011). Detta tesi, assolutamente condivisibile sotto l'ottica della gerarchia delle fonti, non tiene però conto del primo comma dell'art. 16 bis del D.L. 179/2012 che, ad avviso di chi scrive, potrebbe far prevalere la tesi opposta.

Il sopra citato comma 1 dell'art. 16 bis, infatti, stabilisce *"Salvo quanto previsto dal comma 5, a decorrere dal 30 giugno 2014 nei procedimenti civili, contenziosi o di volontaria giurisdizione, innanzi al tribunale,* ***il deposito*** *degli atti processuali e dei documenti da parte dei difensori delle parti precedentemente costituite* ***ha luogo esclusivamente con modalità telematiche, nel rispetto della normativa anche regolamentare concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici.*** *Allo stesso modo si procede per il deposito degli atti e dei documenti da parte dei soggetti nominati o delegati dall'autorità giudiziaria. Le parti provvedono, con le modalità di cui al presente comma a depositare gli atti e i documenti provenienti dai soggetti da esse nominati."*

Quindi, non solo, il comma 1 dell'art. 16 bis richiama espressamente la normativa regolamentare (e quindi implicitamente il D.M. 44/2011 che era già in vigore al momento dell'emanazione del D.L. 179/2012), ma anche lo stesso comma 7 espressamente citando "*Il deposito di cui ai commi da 1 a 4"* del medesimo articolo, altro non fa che riferirsi alla norma appena citata, sancendone l'automatico coordinamento con la normativa di cui all'art. 13 D.M. 44/2011.

Preciso che detta tesi è stata sostenuta recentemente anche da altri Colleghi[69] [70], ma non accolta da tutta la dottrina[71].

Sottoparagrafo 4.3.2. – L'apertura della busta da parte del Cancelliere

Durante l'analisi del flusso dei dati informatici ho sottolineato come l'ultimo passaggio della procedura di deposito sia comunque caratterizzato dal ruolo centrale del personale di Cancelleria.

E' infatti necessario un intervento umano per provvedere allo decompressione e decriptaggio della busta telematica nonché per il successivo deposito di atti e documenti nel fascicolo informatico.

A tal proposito, anche in virtù delle riflessioni – in punto di termini per il deposito – di cui al sottoparagrafo precedente, è emerso sin da subito il problema del momento in cui il Cancelliere provvede materialmente all'analisi della busta telematica.

Certamente la previsione normativa che fa retroagire la data di deposito al momento della generazione della ricevuta di avvenuta consegna (RDAC), farà salvo ogni eventuale sforamento del termine di deposito che derivi da ritardi nell'apertura e gestione del messaggio PEC ma ciò, c'è da sottolinearlo, **unicamente qualora non vi siano errori nel contenuto o nella generazione della busta.**

[69] http://francescominazzi.net/2014/03/07/processo-civile-telematico-trib-milano-ritiene-irrilevante-il-limite-delle-ore-14-per-il-deposito/

[70] http://www.telediritto.it/index.php/processo-telematico/item/128-deposito-telematico-di-una-conclusionale

[71] http://www.altalex.com/index.php?idstr=47&idnot=66734

Nel caso in cui, infatti, avessimo commesso degli errori nell'elaborazione della nostra busta digitale, saremmo obbligatoriamente costretti ad effettuare un nuovo invio e se il termine per il deposito fosse *medio tempore* spirato, non avremmo altra soluzione che richiedere una rimessione in termini al Magistrato di competenza.

Questo è ciò che recentemente è avvenuto presso il Tribunale di Perugia.

In realtà, il caso che stiamo per analizzare, si riferisce ad una problematica attinente all'ufficio di deposito e non tanto ad un errore commesso dal Legale depositante, indi per cui – pur costituendo un importante precedente – non dovrà, ad avviso di chi scrive, invogliare l'Avvocato telematico a depositare il proprio atto digitale il giorno stesso della scadenza del termine[72].

Il 2 gennaio 2014, un Collega appartenente ad un Foro diverso da quello di deposito, provvedeva ad inviare digitalmente una comparsa conclusionale al Tribunale di Perugia.

Il termine per il deposito della memoria era fissato al 7 gennaio 2014 e pertanto il Collega aveva provveduto al deposito con un anticipo di ben 5 giorni.

A seguito delle operazioni di invio erano stati correttamente generati, e a lui consegnati, i primi 3 messaggi dei 4 previsti dalla normativa sul flusso dei dati per il deposito telematico, e quindi, la RDC (ricevuta di accettazione), la RDAC (ricevuta di avvenuta consegna) e l'esito positivo dei controlli formali del Ministero.

Mancava, a quel punto, solo l'intervento del personale di Cancelleria.

La busta *de quo*, però, veniva aperta solo il 9 gennaio 2014 e quindi 2 giorni dopo la scadenza del termine per il deposito.

---

[72] Per un'analisi approfondita del caso di studio si veda l'articolo di Enrico Maria Meco su: "La nuova procedura civile n° 2 anno 2014 http://www.lanuovaproceduracivile.com/wp-content/uploads/2014/03/perugia17_1_14MECO.pdf

L'analisi da parte del Cancelliere dava poi esito negativo, non tanto per problematiche attinenti alla busta telematica ma a causa dell'impossibilità – per il Cancelliere stesso – di ricevere telematicamente le comparse di cui all'art. 190 c.p.c.

Il Tribunale di Perugia infatti, come poi appreso dall'Avvocato depositante, accettava – con valore legale – esclusivamente i ricorsi per decreto ingiuntivo e nessun atto relativo al procedimento civile ordinario.

A seguito della richiesta avanzata dal Collega depositante, il Tribunale di Perugia ha emesso ordinanza di rimessioni in termini in data 17 gennaio 2014[73], ritenendo che la dicitura "accettazione deposito" contenuta nella RDAC (inviata al Legale dal gestore di PEC del Ministero della Giustizia) fosse in effetti idonea a determinare l'errore scusabile in cui il Difensore depositante era incorso in ordine all'avvenuto perfezionamento del deposito della conclusionale.

Ciò detto, va comunque precisato che nella maggior parte dei Tribunali si è provveduto a siglare un accordo con il personale di Cancelleria, al fine di garantire – nei limiti delle possibilità e del carico di lavoro del personale stesso – l'elaborazione delle buste telematiche entro la giornata successiva a quella dell'inoltro tramite PEC, così come è previsto – ad esempio – nelle prassi del Tribunale di Firenze.[74]

[73] Cfr. "La nuova procedura civile n° 2 anno 2014 http://www.lanuovaproceduracivile.com/wp-content/uploads/2014/03/perugia17_1_14.pdf

[74] Art. 23 Protocollo PCT dell'Osservatorio sulla Giustizia Civile di Firenze http://www.osservatoriogiustiziacivilefirenze.it/public/OGCALL_163_0_1.pdf

CAPITOLO 5 – Appendice normativa

Si riportano di seguito, senza alcun carattere di ufficialità, i principali provvedimenti normativi in materia di processo civile telematico.

Paragrafo 5.1 – DECRETO MINISTERIALE 21 febbraio 2011, n. 44.

IL MINISTRO DELLA GIUSTIZIA

di concerto con

IL MINISTRO PER LA PUBBLICA

AMMINISTRAZIONE E L'INNOVAZIONE

Visto l'articolo 17, comma 3, della legge 23 agosto 1988, n. 400;

Visto l'articolo 4 del decreto-legge 29 dicembre 2009, n. 193, recante «Interventi urgenti in materia di funzionalità del sistema giudiziario», convertito in legge, con modificazioni, dalla legge 22 febbraio 2010 n. 24;

Visto il decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali» e successive modificazioni;

Visti gli articoli 16 e 16-bis del decreto-legge 29 novembre 2008, n. 185, recante «Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale», convertito in legge, con modificazioni, dalla legge 28 gennaio 2009, n. 2»;

Visto il decreto del Presidente della Repubblica 13 febbraio 2001, n. 123, recante «Regolamento recante disciplina sull'uso di strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei conti»;

Visto il decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, recante «Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3»;

Visto il decreto del Ministro della giustizia 17 luglio 2008, recante «Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile»;

Visto il decreto ministeriale 27 aprile 2009, recante «Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia»;

Visto il decreto del Presidente del Consiglio dei Ministri 6 maggio 2009, recante «Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini»;

Rilevata la necessità di adottare le regole tecniche previste dall'articolo 4, comma 1, del citato decreto, in sostituzione delle regole tecniche adottate con il decreto del Presidente della Repubblica 13 febbraio 2001, n. 123 e con il decreto del Ministro della giustizia 17 luglio 2008;

Acquisito il parere espresso in data 15 luglio 2010 dal Garante per la protezione dei dati personali;

Acquisito il parere espresso in data 20 luglio 2010 da DigitPA;

Udito il parere del Consiglio di Stato, espresso dalla sezione consultiva per gli atti normativi nell'adunanza del 25 novembre 2010 e quello espresso nell'adunanza del 20 dicembre 2010;

Vista la comunicazione al Presidente del Consiglio dei Ministri in data 18 gennaio 2011;

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 dominio giustizia, che consente l'interoperabilità tra i sistemi informatici utilizzati dai soggetti abilitati interni, il portale dei servizi telematici e il gestore di posta elettronica certificata del Ministero della giustizia;

e) posta elettronica certificata: sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici, di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68;

f) identificazione informatica: operazione di identificazione in rete del titolare della carta nazionale dei servizi o di altro dispositivo crittografico, mediante un certificato di autenticazione, secondo la definizione di cui al decreto legislativo 7 marzo 2005, n. 82;

g) firma digitale: firma elettronica avanzata, basata su un certificato qualificato, rilasciato da un certificatore accreditato, e generata mediante un dispositivo per la creazione di una firma sicura, di cui al decreto legislativo 7 marzo 2005, n. 82;

h) fascicolo informatico: versione informatica del fascicolo d'ufficio, contenente gli atti del processo come documenti informatici, oppure le copie informatiche dei medesimi atti, qualora siano stati depositati su supporto cartaceo, ai sensi del codice dell'amministrazione digitale;

i) codice dell'amministrazione digitale (CAD): decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni;

l) codice in materia di protezione dei dati personali: decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" e successive modificazioni;

m) soggetti abilitati: i soggetti abilitati all'utilizzo dei servizi di consultazione di informazioni e trasmissione di documenti informatici relativi al processo. In particolare si intende per:

1) soggetti abilitati interni: i magistrati, il personale degli uffici giudiziari e degli UNEP;

2) soggetti abilitati esterni: i soggetti abilitati esterni privati e i soggetti abilitati esterni pubblici;

3) soggetti abilitati esterni privati: i difensori delle parti private, gli avvocati iscritti negli elenchi speciali, gli esperti e gli ausiliari del giudice;

4) soggetti abilitati esterni pubblici: gli avvocati, i procuratori dello Stato e gli altri dipendenti di amministrazioni statali, regionali, metropolitane, provinciali e comunali;

n) utente privato: la persona fisica o giuridica, quando opera al di fuori dei casi previsti dalla lettera m);

o) certificazione del soggetto abilitato esterno privato: attestazione di iscrizione all'albo, all'albo speciale, al registro ovvero di possesso della qualifica che legittima l'esercizio delle funzioni professionali e l'assenza di cause ostative all'accesso;

p) certificazione del soggetto abilitato esterno pubblico: attestazione di appartenenza del soggetto all'amministrazione pubblica e dello svolgimento di funzioni tali da legittimare l'accesso;

q) specifiche tecniche: le disposizioni di carattere tecnico emanate, ai sensi dell'articolo 34, dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia, sentito DigitPA e il Garante per la protezione dei dati personali, limitatamente ai profili inerenti la protezione dei dati personali;

r) spam: messaggi indesiderati;

s) software antispam: software studiato e progettato per rilevare ed eliminare lo spam;

t) log: documento informatico contenente la registrazione cronologica di una o più operazioni informatiche, generato automaticamente dal sistema informatico;

u) richiesta di pagamento telematico (RPT): struttura standardizzata che definisce gli elementi necessari a caratterizzare il pagamento e qualifica il versamento con un identificativo univoco, nonché contiene i dati identificativi, variabili secondo il tipo di operazione, e una parte riservata per inserire informazioni elaborabili automaticamente dai sistemi informatici;

v) ricevuta telematica (RT): struttura standardizzata, emessa a fronte di una RPT, che definisce gli elementi necessari a qualificare il pagamento e trasferisce inalterate le informazioni della RPT relative alla parte riservata;

z) identificativo univoco di erogazione del servizio (CRS): identifica univocamente una richiesta di erogazione del servizio ed 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 sicurezza di cui all'articolo 26.

6. Il portale dei servizi telematici consente accesso senza l'impiego di apposite credenziali, sistemi di identificazione e requisiti di legittimazione, alle informazioni ed

alla documentazione sui servizi telematici del dominio giustizia, alle raccolte giurisprudenziali e alle informazioni essenziali sullo stato dei procedimenti pendenti, che vengono rese disponibili in forma anonima.

Art. 7 Registro generale degli indirizzi elettronici

1. Il registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia, contiene i dati identificativi e l'indirizzo di posta elettronica certificata dei soggetti abilitati esterni di cui al comma 3 e degli utenti privati di cui al comma 4.

2. Per i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato, il registro generale degli indirizzi elettronici 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, raccogliendo in un fascicolo informatico gli atti, i documenti, gli allegati, le ricevute di posta elettronica certificata e i dati del procedimento medesimo da chiunque formati, ovvero le copie informatiche dei medesimi atti quando siano stati depositati su supporto cartaceo.

2. Il sistema di gestione del fascicolo informatico è la parte del sistema documentale del Ministero della giustizia dedicata all'archiviazione e al reperimento di tutti i documenti informatici, prodotti sia all'interno che all'esterno, secondo le specifiche tecniche di cui all'articolo 34.

3. La tenuta e conservazione del fascicolo informatico equivale alla tenuta e conservazione del fascicolo d'ufficio su supporto cartaceo, fermi restando gli obblighi di conservazione dei documenti originali unici su supporto cartaceo previsti dal codice dell'amministrazione digitale e dalla disciplina processuale vigente.

4. Il fascicolo informatico reca l'indicazione:

a) dell'ufficio titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;

b) dell'oggetto del procedimento;

c) dell'elenco dei documenti contenuti.

5. Il fascicolo informatico è formato in modo da garantire la facile reperibilità ed il collegamento degli atti ivi contenuti in relazione alla data di deposito, al loro contenuto, ed alle finalità dei singoli documenti.

6. Con le specifiche tecniche di cui all'articolo 34 sono definite le modalità per il salvataggio dei log relativi alle operazioni di accesso al fascicolo informatico.

Art. 10 Infrastruttura di comunicazione

1. I sistemi informatici del dominio giustizia utilizzano l'infrastruttura tecnologica resa disponibile nell'ambito del Sistema Pubblico di Connettività per le comunicazioni con l'esterno del dominio giustizia.

CAPO III

Trasmissione di atti e documenti informatici

Art. 11 Formato dell'atto del processo in forma di documento informatico

1. L'atto del processo in forma di documento informatico è privo di elementi attivi ed è redatto nei formati previsti dalle specifiche tecniche di cui all'articolo 34; le informazioni strutturate sono in formato XML, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, pubblicate sul portale dei servizi telematici.

2. La nota di iscrizione a ruolo può essere trasmessa per via telematica come documento informatico sottoscritto con firma digitale; le relative informazioni sono contenute nelle informazioni strutturate di cui al primo comma, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

Art. 12 Formato dei documenti informatici allegati

1. I documenti informatici allegati all'atto del processo sono privi di elementi attivi e hanno i formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34.

2. È consentito l'utilizzo dei formati compressi, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, purché contenenti solo file nei formati previsti dal comma precedente.

Art. 13 Trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati

1. I documenti informatici di cui agli articoli 11 e 12 sono trasmessi da parte dei soggetti abilitati esterni e degli utenti privati mediante l'indirizzo di posta elettronica certificata risultante dal registro generale degli indirizzi elettronici, all'indirizzo di posta elettronica certificata dell'ufficio destinatario, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2. I documenti informatici di cui al comma 1 si intendono ricevuti dal dominio giustizia nel momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del Ministero della giustizia.

3. Nel caso previsto dal comma 2 la ricevuta di avvenuta consegna attesta, altresì, l'avvenuto deposito dell'atto o del documento presso l'ufficio giudiziario competente. Quando la ricevuta è rilasciata dopo le ore 14 il deposito si considera effettuato il giorno feriale immediatamente successivo.

4. Il rigetto del deposito da parte dell'ufficio non impedisce il successivo deposito entro i termini assegnati o previsti dalla vigente normativa processuale.

5. La certificazione dei professionisti abilitati e dei soggetti abilitati esterni pubblici è effettuata dal gestore dei servizi telematici sulla base dei dati presenti nel registro generale degli indirizzi elettronici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

6. Al fine di garantire la riservatezza dei documenti da trasmettere, il soggetto abilitato esterno utilizza un meccanismo di crittografia, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

7. Il gestore dei servizi telematici restituisce al mittente l'esito dei controlli effettuati dal dominio giustizia nonché dagli operatori della cancelleria o della segreteria, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

8. La dimensione massima del messaggio è stabilita nelle specifiche tecniche di cui all'articolo 34. Se il messaggio eccede tale dimensione, il gestore dei servizi telematici genera e invia automaticamente al mittente un messaggio di errore, contenente l'avviso del rifiuto del messaggio, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

9. I soggetti abilitati esterni possono avvalersi dei servizi del punto di accesso, di cui all'articolo 23, per la trasmissione dei documenti; in tale caso il punto di accesso si attiene alle modalità di trasmissione dei documenti di cui al presente articolo.

Art. 14 Documenti probatori e allegati non informatici

1. I documenti probatori e gli allegati depositati in formato non elettronico sono identificati e descritti in una apposita sezione delle informazioni strutturate di cui all'articolo 11, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2. La cancelleria o la segreteria dell'ufficio giudiziario provvede ad effettuare copia informatica dei documenti probatori e degli allegati su supporto cartaceo e ad inserirla nel fascicolo informatico, apponendo la firma digitale ai sensi e per gli effetti di cui all'articolo 22, comma 3 del codice dell'amministrazione digitale.

Art. 15 Deposito dell'atto del processo da parte dei soggetti abilitati interni

1. L'atto del processo, redatto in formato elettronico da un soggetto abilitato interno e sottoscritto con firma digitale, è depositato telematicamente nel fascicolo informatico.

2. In caso di atto formato da organo collegiale l'originale del provvedimento è sottoscritto con firma digitale anche dal presidente.

3. Quando l'atto è redatto dal cancelliere o dal segretario dell'ufficio giudiziario questi vi appone la propria firma digitale e ne effettua il deposito nel fascicolo informatico.

4. Se il provvedimento del magistrato è in formato cartaceo, il cancelliere o il segretario dell'ufficio giudiziario ne estrae copia informatica nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34 e provvede a depositarlo nel fascicolo informatico, apponendovi la propria firma digitale.

Art. 16 Comunicazioni per via telematica

1. La comunicazione per via telematica dall'ufficio giudiziario ad un soggetto abilitato esterno o all'utente privato avviene mediante invio di un messaggio dall'indirizzo di posta elettronica certificata dell'ufficio giudiziario mittente all'indirizzo di posta elettronica certificata del destinatario, indicato nel registro generale degli indirizzi elettronici, ovvero per la persona fisica consultabile ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 e per l'impresa indicato nel registro delle imprese, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2. La cancelleria o la segreteria dell'ufficio giudiziario provvede ad effettuare una copia informatica dei documenti cartacei da comunicare nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34, che conserva nel fascicolo informatico.

3. La comunicazione per via telematica si intende perfezionata nel momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del destinatario e produce gli effetti di cui agli articoli 45 e 48 del codice dell'amministrazione digitale. (6)

4. Fermo quanto previsto dall'articolo 20, comma 6, e salvo il caso fortuito o la forza maggiore, negli uffici giudiziari individuati con il decreto di cui all'articolo 51, comma 3 del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, nel caso in cui viene generato un avviso di mancata consegna previsto dalle regole tecniche della posta elettronica certificata, si procede ai sensi del comma 3 del medesimo articolo 51 e viene pubblicato nel portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, un apposito avviso di avvenuta comunicazione o notificazione dell'atto nella cancelleria o segreteria dell'ufficio giudiziario, contenente i soli elementi identificativi del procedimento e delle parti e loro patrocinatori. Tale avviso è visibile solo dai soggetti abilitati esterni legittimati ai sensi dell'articolo 27, comma 1, del decreto ministeriale 21 febbraio 2011, n. 44.

5. Le ricevute di avvenuta consegna e gli avvisi di mancata consegna vengono conservati nel fascicolo informatico.

6. La comunicazione che contiene dati sensibili è effettuata per estratto con contestuale messa a disposizione dell'atto integrale nell'apposita area del portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34 e nel rispetto dei requisiti di sicurezza di cui all'articolo 26, con modalità tali da garantire l'identificazione dell'autore dell'accesso e la tracciabilità delle relative attività.

7. Nel caso previsto dal comma 6, si applicano le disposizioni di cui ai commi 2 e 3, ma la comunicazione si intende perfezionata il giorno feriale successivo al momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del destinatario.

8. Si applica, in ogni caso, il disposto dell'articolo 49 del codice dell'amministrazione digitale.

Art. 17 Notificazioni per via telematica

1. Al di fuori dei casi previsti dall'articolo 51, del decreto-legge 25 giugno 2008, n. 112, convertito con modificazioni dalla legge 6 agosto 2008, n. 133, e successive modificazioni, le richieste telematiche di un'attività di notificazione da parte di un ufficio giudiziario sono inoltrate al sistema informatico dell'UNEP, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2. Le richieste di altri soggetti sono inoltrate all'UNEP tramite posta elettronica certificata, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

3. La notificazione per via telematica da parte dell'UNEP rispetta i requisiti richiesti per la comunicazione da un ufficio giudiziario verso i soggetti abilitati esterni di cui all'articolo 16.

4. Il sistema informatico dell'UNEP individua l'indirizzo di posta elettronica del destinatario dal registro generale degli indirizzi elettronici, dal registro delle imprese o dagli albi o elenchi costituiti ai sensi dell'articolo 16 del decreto-legge 29 novembre 2008, n. 185 convertito con modificazioni dalla legge 28 gennaio 2009, n. 2, nonché per il cittadino dall'elenco reso consultabile ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei Ministri 6 maggio 2009 in base alle specifiche tecniche stabilite ai sensi dell'articolo 34.

5. Il sistema informatico dell'UNEP, eseguita la notificazione, trasmette per via telematica a chi ha richiesto il servizio il documento informatico con la relazione di notificazione sottoscritta mediante firma digitale e congiunta all'atto cui si riferisce, nonché le ricevute di posta elettronica certificata, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

6. L'ufficiale giudiziario, se non procede alla notificazione per via telematica, effettua la copia cartacea del documento informatico, attestandone la conformità all'originale, e provvede a notificare la copia stessa con le modalità previste dalla normativa processuale vigente.

Art. 18 Notificazioni per via telematica eseguite dagli avvocati

1. L'avvocato che procede alla notificazione con modalità telematica ai sensi dell'articolo 3-bis della legge 21 gennaio 1994, n. 53, allega al messaggio di posta elettronica certificata documenti informatici o copie informatiche, anche per immagine, di documenti analogici privi di elementi attivi e redatti nei formati consentiti dalle specifiche tecniche stabilite ai sensi dell'articolo 34.

2. Quando il difensore procede alla notificazione delle comparse o delle memorie, ai sensi dell'articolo 170, quarto comma, del codice di procedura civile, la notificazione è effettuata mediante invio della memoria o della comparsa alle parti costituite ai sensi del comma 1.

3. La parte rimasta contumace ha diritto a prendere visione degli atti del procedimento tramite accesso al portale dei servizi telematici e, nei casi previsti, anche tramite il punto di accesso.

4. L'avvocato che estrae copia informatica per immagine dell'atto formato su supporto analogico, compie l'asseverazione prevista dall'articolo 22, comma 2, del codice dell'amministrazione digitale, inserendo la dichiarazione di conformità all'originale nella relazione di notificazione, a norma dell'articolo 3-bis, comma 5, della legge 21 gennaio 1994, n. 53.

5. La procura alle liti si considera apposta in calce all'atto cui si riferisce quando è rilasciata su documento informatico separato allegato al messaggio di posta elettronica certificata mediante il quale l'atto è notificato. La disposizione di cui al periodo precedente si applica anche quando la procura alle liti è rilasciata su foglio separato del quale è estratta copia informatica, anche per immagine.

6. La ricevuta di avvenuta consegna prevista dall'articolo 3-bis, comma 3, della legge 21 gennaio 1994, n. 53 è quella completa, di cui all'articolo 6, comma 4, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68.

Art. 19 Disposizioni particolari per la fase delle indagini preliminari

1. Nelle indagini preliminari le comunicazioni tra l'ufficio del pubblico ministero e gli ufficiali ed agenti di polizia giudiziaria avvengono su canale sicuro protetto da un meccanismo di crittografia secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2. Le specifiche tecniche assicurano l'identificazione dell'autore dell'accesso e la tracciabilità delle relative attività, anche mediante l'utilizzo di misure di sicurezza ulteriori rispetto a quelle previste dal disciplinare tecnico di cui all'allegato B del codice in materia di protezione dei dati personali.

3. Per le comunicazioni di atti e documenti del procedimento di cui al comma 1 sono utilizzati i gestori di posta elettronica certificata delle forze di polizia. Gli indirizzi di posta elettronica certificata sono resi disponibili unicamente agli utenti abilitati sulla base delle specifiche stabilite ai sensi dell'articolo 34.

4. Alle comunicazioni previste dal presente articolo si applicano, in quanto compatibili, le disposizioni dell'articolo 16, commi 1, 2, 3, 4 e 5, e dell'articolo 20.

5. L'atto del processo in forma di documento informatico è privo di elementi attivi ed è redatto dalle forze di polizia nei formati previsti dalle specifiche tecniche stabilite ai sensi dell'articolo 34; le informazioni strutturate sono in formato XML, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34. L'atto del processo, protetto da meccanismi di crittografia, è sottoscritto con firma digitale. Si applicano, in quanto compatibili, l'articolo 14 del presente decreto, nonché gli articoli 20 e 21 del codice dell'amministrazione digitale.

6. La comunicazione degli atti del processo alle forze di polizia, successivamente al deposito previsto dall'articolo 15, è effettuata per estratto con contestuale messa a disposizione dell'atto integrale, protetto da meccanismo di crittografia, in apposita area riservata all'interno del dominio giustizia, accessibile solo dagli appartenenti alle forze di polizia legittimati, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34 e nel rispetto dei requisiti di sicurezza di cui all'articolo 26.

7. Per la gestione del fascicolo informatico si applicano, in quanto compatibili, le disposizioni di cui all'articolo 9, commi da 1 a 5. Agli atti contenuti nel fascicolo informatico, custodito in una sezione distinta del sistema documentale di cui all'articolo 9, protetta da un meccanismo di crittografia secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, hanno accesso unicamente i soggetti abilitati interni appositamente abilitati. Alla conclusione delle indagini preliminari, e in ogni altro caso in cui il fascicolo o parte di esso deve essere consultato da soggetti abilitati esterni o da utenti privati, questi accedono alla copia resa disponibile mediante il punto di accesso e il portale dei servizi telematici, secondo quanto previsto al capo IV.

8. Per la trasmissione telematica dei flussi informativi sintetici delle notizie di reato e dei relativi esiti tra il Centro Elaborazione Dati del Servizio per il Sistema Informativo Interforze, di cui all'articolo 8, della legge 1° aprile 1981, n. 121 e successive modifiche ed integrazioni, e il sistema dei registri delle notizie di reato delle Procure della Repubblica sono utilizzate le infrastrutture di connettività delle pubbliche amministrazioni che consentono una interconnessione tra le Amministrazioni, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34. Il canale di comunicazione è protetto con le modalità di cui al comma 1.

9. Per assicurare la massima riservatezza della fase delle indagini preliminari la base di dati dei registri di cui al comma 8 è custodita, con le speciali misure di cui al comma 2, separatamente rispetto a quella relativa ai procedimenti per i quali è stato emesso uno degli atti di cui all'articolo 60, del codice di procedura penale, in infrastrutture informatiche di livello distrettuale o interdistrettuale individuate dal responsabile per i sistemi informativi automatizzati. I compiti di vigilanza sulle procedure di sicurezza adottate sulla base dati prevista dal presente comma sono svolti dal Procuratore della Repubblica presso il Tribunale e dal Procuratore generale della Repubblica presso la Corte di appello competenti in relazione all'ufficio giudiziario titolare dei dati, avvalendosi del personale tecnico individuato dal responsabile per i sistemi informativi automatizzati.

Art. 20 Requisiti della casella di PEC del soggetto abilitato esterno

1. Il gestore di posta elettronica certificata del soggetto abilitato esterno, fermi restando gli obblighi previsti dal decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 e dal decreto ministeriale 2 novembre 2005, recante «Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata», è

tenuto ad adottare software antispam idoneo a prevenire la trasmissione di messaggi di posta elettronica indesiderati.

2. Il soggetto abilitato esterno è tenuto a dotare il terminale informatico utilizzato di software idoneo a verificare l'assenza di virus informatici per ogni messaggio in arrivo e in partenza e di software antispam idoneo a prevenire la trasmissione di messaggi di posta elettronica indesiderati.

3. Il soggetto abilitato esterno è tenuto a conservare, con ogni mezzo idoneo, le ricevute di avvenuta consegna dei messaggi trasmessi al dominio giustizia.

4. La casella di posta elettronica certificata deve disporre di uno spazio disco minimo definito nelle specifiche tecniche di cui all'articolo 34.

5. Il soggetto abilitato esterno è tenuto a dotarsi di servizio automatico di avviso dell'imminente saturazione della propria casella di posta elettronica certificata e a verificare l'effettiva disponibilità dello spazio disco a disposizione.

6. La modifica dell'indirizzo elettronico può avvenire dal 1° al 31 gennaio e dal 1° al 31 luglio.

7. La disposizione di cui al comma 6 non si applica qualora la modifica dell'indirizzo si renda necessaria per cessazione dell'attività da parte del gestore di posta elettronica certificata.

Art. 21 Richiesta delle copie di atti e documenti

1. Il rilascio della copia di atti e documenti del processo avviene, previa verifica del regolare pagamento dei diritti previsti, tramite invio all'indirizzo di posta elettronica certificata del richiedente, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2. L'atto o il documento che contiene dati sensibili o di grandi dimensioni è messo a disposizione nell'apposita area del portale dei servizi telematici, nel rispetto dei requisiti di sicurezza stabiliti ai sensi dell'articolo 34.

3. Nel caso di richiesta di copia informatica, anche parziale, conforme al documento originale in formato cartaceo, il cancelliere ne attesta la conformità all'originale sottoscrivendola con la propria firma digitale.

CAPO IV

Consultazione delle informazioni del dominio giustizia

Art. 22 Servizi di consultazione

1. Ai fini di cui agli articoli 50, comma 1, 52 e 56 del codice dell'amministrazione digitale, l'accesso ai servizi di consultazione delle informazioni rese disponibili dal dominio giustizia avviene tramite un punto di accesso o tramite il portale dei servizi telematici, nel rispetto dei requisiti di sicurezza di cui all'articolo 26.

Art. 23 Punto di accesso

1. Il punto di accesso può essere attivato esclusivamente dai soggetti indicati dai commi 6 e 7.

2. Il punto di accesso fornisce un'adeguata qualità dei servizi, dei processi informatici e dei relativi prodotti, idonea a garantire la sicurezza del sistema, nel rispetto dei requisiti tecnici di cui all'articolo 26.

3. Il punto di accesso fornisce adeguati servizi di formazione e assistenza ai propri utenti, anche relativamente ai profili tecnici.

4. La violazione da parte del gestore di un punto di accesso dei livelli di sicurezza e di servizio comporta la sospensione dell'autorizzazione ad erogare i servizi fino al ripristino di tali livelli.

5. Il Ministero della giustizia dispone ispezioni tecniche, anche a campione, per verificare l'attuazione delle prescrizioni di sicurezza.

6. Possono gestire uno o più punti di accesso:

a) i consigli degli ordini professionali, i collegi ed i Consigli nazionali professionali, limitatamente ai propri iscritti;

b) il Consiglio nazionale forense, ove delegato da uno o più consigli degli ordini degli avvocati, limitatamente agli iscritti del consiglio delegante;

c) il Consiglio nazionale del notariato, limitatamente ai propri iscritti;

d) l'Avvocatura dello Stato, le amministrazioni statali o equiparate, e gli enti pubblici, limitatamente ai loro iscritti e dipendenti;

e) le Regioni, le città metropolitane, le provincie ed i Comuni, o enti consorziati tra gli stessi;

f) Le Camere di Commercio, per le imprese iscritte nel relativo registro.

7. I punti di accesso possono essere altresì gestiti da società di capitali in possesso di un capitale sociale interamente versato non inferiore a un milione di euro.

Art. 24 Elenco pubblico dei punti di accesso

1. L'elenco pubblico dei punti di accesso attivi presso il Ministero della giustizia comprende le seguenti informazioni:

a) identificativo del punto di accesso;

b) sede legale del soggetto titolare del punto di accesso;

c) indirizzo internet;

d) dati relativi al legale rappresentante del punto di accesso o a un suo delegato, comprendenti: nome, cognome, codice fiscale, indirizzo di posta elettronica certificata, numero di telefono e di fax;

e) recapiti relativi ai referenti tecnici da contattare in caso di problemi.

Art. 25 Iscrizione nell'elenco pubblico dei punti di accesso

1. Il soggetto che intende costituire un punto di accesso inoltra domanda di iscrizione nell'elenco pubblico dei punti di accesso secondo il modello e con le modalità stabilite dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia con apposito decreto, da adottarsi entro sessanta giorni dall'entrata in vigore del presente decreto.

2. Il Ministero della giustizia decide sulla domanda entro trenta giorni, con provvedimento motivato, anche sulla base di apposite verifiche, effettuabili anche da personale esterno all'Amministrazione, da questa delegato, con costi a carico del richiedente.

3. Con il provvedimento di cui al comma 2, il Ministero della giustizia delega la responsabilità del processo di identificazione dei soggetti abilitati esterni al punto di accesso. Il Ministero della giustizia può delegare la responsabilità del processo di identificazione degli utenti privati agli enti pubblici di cui all'articolo 23, comma 6, lettera e).

4. Il Ministero della giustizia può verificare l'adempimento degli obblighi assunti da parte del gestore del punto di accesso di propria iniziativa oppure su segnalazione. In caso di violazione si applicano le disposizioni di cui all'articolo 23, comma 3.

Art. 26 Requisiti di sicurezza

1. L'accesso ai servizi di consultazione delle informazioni rese disponibili dal dominio giustizia avviene mediante identificazione sul punto di accesso o sul portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

2. Il punto di accesso stabilisce la connessione con il portale dei servizi telematici mediante un collegamento sicuro con mutua autenticazione secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

3. A seguito dell'identificazione viene in ogni caso trasmesso al gestore dei servizi telematici il codice fiscale del soggetto che effettua l'accesso.

4. I punti di accesso garantiscono un'adeguata sicurezza del sistema con le modalità tecniche specificate in un apposito piano depositato unitamente all'istanza di cui all'articolo 25, a pena di inammissibilità della stessa.

Art. 27 Visibilità delle informazioni

1. Ad eccezione della fase di cui all'articolo 19, il dominio giustizia consente al soggetto abilitato esterno l'accesso alle informazioni contenute nei fascicoli dei procedimenti in cui è costituito o svolge attività di esperto o ausiliario. L'utente privato accede alle informazioni contenute nei fascicoli dei procedimenti in cui è parte mediante il portale dei servizi telematici e, nei casi previsti dall'articolo 23, comma 6, lettere e) ed f), e comma 7, mediante il punto di accesso.

2. 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 autorizzato o presso il portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, comma 1.

2. I punti di accesso trasmettono al Ministero della giustizia le informazioni relative ad i propri utenti registrati, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, comma 1.

Art. 29 Orario di disponibilità dei servizi di consultazione

1. Il portale dei servizi telematici e il gestore dei servizi telematici garantiscono la disponibilità dei servizi secondo le specifiche tecniche stabilite ai sensi dell'articolo 34. In ogni caso è garantita la disponibilità dei servizi di consultazione nei giorni feriali dalle ore otto alle ore ventidue, dal lunedì al venerdì, e dalle ore otto alle ore tredici del sabato e dei giorni ventiquattro e trentun dicembre.

CAPO V

Pagamenti telematici

Art. 30 Pagamenti

1. Il pagamento del contributo unificato e degli altri diritti e spese è effettuato nelle forme previste dal decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni. La ricevuta e l'attestazione di pagamento o versamento è allegata alla nota di iscrizione a ruolo o ad altra istanza inviata all'ufficio, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34, ed è conservata dall'interessato per essere esibita a richiesta dell'ufficio.

2. Il pagamento di cui al comma 1 può essere effettuato per via telematica con le modalità e gli strumenti previsti dal decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni e dalle altre disposizioni normative e regolamentari relative al riversamento delle entrate alla Tesoreria dello Stato.

3. L'interazione tra le procedure di pagamento telematico messe a disposizione dal prestatore del servizio di pagamento, il punto di accesso e il portale dei servizi telematici avviene su canale sicuro, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

4. Il processo di pagamento telematico assicura l'univocità del pagamento mediante l'utilizzo della richiesta di pagamento telematico (RPT), della ricevuta telematica (RT) e dell'identificativo univoco di erogazione del servizio (CRS) che impediscono, mediante l'annullamento del CRS, un secondo utilizzo della RT. Le specifiche tecniche sono definite ai sensi dell'articolo 34.

5. La ricevuta telematica, firmata digitalmente dal prestatore del servizio di pagamento che effettua la riscossione o da un soggetto da questo delegato, costituisce prova del pagamento alla Tesoreria dello Stato ed è conservata nel fascicolo informatico.

6. L'ufficio verifica periodicamente con modalità telematiche la regolarità delle ricevute o attestazioni e il buon esito delle transazioni di pagamento telematico.

Art. 31 Diritto di copia

1. L'interessato, all'atto della richiesta di copia, richiede l'indicazione dell'importo del diritto corrispondente che gli è comunicato senza ritardo con mezzi telematici dall'ufficio, secondo le specifiche stabilite ai sensi dell'articolo 34.

2. Alla richiesta di copia è associato un identificativo univoco che, in caso di pagamento dei diritti di copia non contestuale, viene evidenziato nel sistema informatico per consentire il versamento secondo le modalità previste dal decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni.

3. La ricevuta telematica è associata all'identificativo univoco.

Art. 32 Registrazione, trascrizione e voltura degli atti

1. La registrazione, la trascrizione e la voltura degli atti avvengono in via telematica nelle forme previste dall'articolo 73 del decreto del Presidente della Repubblica 30 maggio 2002, n. 115, e successive modificazioni.

Art. 33 Pagamento dei diritti di notifica

1. Il pagamento dei diritti di notifica viene effettuato nelle forme previste dall'articolo 30.

2. L'UNEP rende pubblici gli importi dovuti a titolo di anticipazione. Eseguita la notificazione, l'UNEP comunica l'importo definitivo e restituisce il documento informatico notificato previo versamento del conguaglio dovuto dalla parte oppure unitamente al rimborso del maggior importo versato in acconto.

CAPO VI

Disposizioni finali e transitorie

Art. 34 Specifiche tecniche

1. Le specifiche tecniche sono stabilite dal responsabile per i sistemi informativi automatizzati del Ministero della giustizia, sentito DigitPA e, limitatamente ai profili inerenti alla protezione dei dati personali, sentito il Garante per la protezione dei dati personali.

2. Le specifiche di cui al comma precedente vengono rese disponibili mediante pubblicazione nell'area pubblica del portale dei servizi telematici.

3. Fino all'emanazione delle specifiche tecniche di cui al comma 1, continuano ad applicarsi, in quanto compatibili, le disposizioni anteriormente vigenti.

Art. 35 Disposizioni finali e transitorie

1. L'attivazione della trasmissione dei documenti informatici da parte dei soggetti abilitati esterni è preceduta da un decreto dirigenziale che accerta l'installazione e l'idoneità delle attrezzature informatiche, unitamente alla funzionalità dei servizi di comunicazione dei documenti informatici nel singolo ufficio.

2. L'indirizzo elettronico già previsto dal decreto del Ministro della giustizia 17 luglio 2008, recante «Regole tecnico-operative per l'uso di strumenti informatici e telematici nel processo civile» è utilizzabile per un periodo transitorio non superiore a sei mesi dalla data di entrata in vigore del presente decreto.

3. La data di attivazione dell'indirizzo di posta elettronica certificata di cui all'articolo 4, comma 2, 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 strutturazione dei modelli informatici sono definite con decreto del responsabile per i sistemi informativi automatizzati del Ministero della giustizia e pubblicate nell'area pubblica del portale dei servizi telematici.

5. Fino all'emanazione dei provvedimenti di cui al comma 4, conservano efficacia le caratteristiche di strutturazione dei modelli informatici di cui al decreto del Ministro della giustizia 10 luglio 2009, recante "Nuova strutturazione dei modelli informatici relativa all'uso di strumenti informatici e telematici nel processo civile e introduzione dei modelli informatici per l'uso di strumenti informatici e telematici nelle procedure esecutive individuali e concorsuali", pubblicato nella Gazzetta Ufficiale n. 165 del 18 luglio 2009 - S.O. n. 120.

Art. 36 Adeguamento delle regole tecnico-operative

1. Le regole tecnico-operative sono adeguate all'evoluzione scientifica e tecnologica, con cadenza almeno biennale, a decorrere dalla data di entrata in vigore del presente decreto.

Art. 37 Efficacia

1. Il presente decreto acquista efficacia il trentesimo giorno successivo a quello della sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana

2. Dalla data di cui al comma 1, cessano di avere efficacia nel processo civile le disposizioni del decreto del Presidente della Repubblica 13 febbraio 2001, n. 123 e del decreto del Ministro della giustizia 17 luglio 2008.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Paragrafo 5.2 – Provvedimento 16 aprile 2014

MINISTERO DELLA GIUSTIZIA

PROVVEDIMENTO 16 aprile 2014.

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.

IL RESPONSABILE PER I SISTEMI INFORMATIVI AUTOMATIZZATI

DELLA DIREZIONE GENERALE 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 201 1), 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", come modificato dal decreto ministeriale 15 ottobre 2012 n. 209 e dal decreto ministeriale 3 aprile 2013 n. 48;

Visto il decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221 e successivamente modificato dalla legge 24 dicembre 2012, n. 228;

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali» e successive modificazioni;

Visto il decreto del Presidente della Repubblica 1 1 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 Presidente del Consiglio dei ministri 22 febbraio 2013;

Visto il decreto ministeriale 27 aprile 2009, recante «Nuove regole procedurali relative alla tenuta dei registri informatizzati dell'amministrazione della giustizia»;

Rilevata la necessita di aggiornare le specifiche tecniche previste dall'articolo 34, comma 1, del citato decreto ministeriale 21 febbraio 2011, n. 44;

Acquisito il parere espresso in data 23 dicembre 2013 dal Garante per la protezione dei dati personali;

Acquisito il parere espresso in data 4 febbraio 2014 dall'Agenzia per l'Italia Digitale;

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 pre-visti dal decreto legislativo 7 marzo 2005, n. 82, e successive modifica-zioni, 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" e successive modificazioni;

   b) CAD: codice dell'amministrazione digitale (decreto legislativo 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" e successive modificazioni);

   c) CNS: Carta Nazionale dei Servizi;

d) CSV: Comma-separated values;

e) DTD: Document Type Definition;

f) DGSIA: Direzione Generale per i Sistemi Informativi Automatizzati del Ministero della Giustizia;

g) GSU: Sistema di gestione informatizzata dei registri per gli uffici notifi-che 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 Marlcup 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 apposita sequenza di chiamate al token per mezzo dell'interfaccia PKCS#1 1 è possibile implementare la procedura di identificazione;

y) CAdES (CMS Advanced Electronic Signature): formato di busta crittografica definito nella norma ETSI TS 101 733 V1.7.4 e basata a sua volta sulle specifiche RFC 3852 e RFC 2634 e successive modificazioni;

z) PAdES (PDF Advanced Electronic Signature): formato di busta crittografica definito nella norma ETSI TS 102 778 basata a sua volta sullo standard ISO/IEC 32000 e successive modificazioni;

aa) OID (Object IDentifier): codice univoco basato su una sequenza ordinata di numeri per l'identificazione di evidenze informatiche utilizzate per la rappresentazione di oggetti come estensioni, attributi, documenti e strutture di dati in genere nell'ambito degli standard internazionali re-lativi alla interconnessione dei sistemi aperti che richiedono un'identificazione univoca in ambito mondiale;

bb) Autenticazione a due fattori: metodo di autenticazione che si basa sull'utilizzo congiunto di due metodi di autenticazione individuale, ossia che combina un'informazione nota (ad esempio un nome utente e una password) con un oggetto a disposizione (ad esempio, una carta di credito, token o telefono cellulare).

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 nazionale, interdistrettuale e distrettuale. In fase transitoria e quando ragioni tecniche lo rendono assolutamente necessario, possono essere mantenute strutture a livello locale (di circondario).

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, oppure presso una sala server del Ministero della giustizia.

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 Direttore Generale 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 ca-so 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 re-golamento, nel rispetto delle specifiche tecniche riportate nel presente provvedimento.

2. Le caselle appartengono ad apposito sotto-dominio (civile.ptel.giustiziacert.it e penale.ptel.giustiziacert.it) e possono ricevere uni-camente messaggi di posta elettronica certificata. I messaggi di posta elet-tronica 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 caselle di PEC diverse da quelle di cui ai commi precedenti 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 cinque 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 servi ce 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 abilita-ti; in questo caso il gestore dei servizi telematici utilizza un canale sicuro protetto 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 http://pst.giustizia.it ed è composto di una "area pubblica" e di una "area riservata".

2. L'"area pubblica", denominata "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 risali-re 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 per i soggetti abilitati esterni e gli utenti priva-ti avviene sul portale dei servizi telematici mediante carta d'identità elettro-nica o carta nazionale dei servizi e sul punto di accesso mediante autenti-cazione a due fattori oppure tramite token crittografico (smart card, chia-vetta USB o altro dispositivo sicuro) in conformità all'articolo 64 del decreto legislativo 7 marzo 2005, n. 82; in caso si utilizzi il token crittografico, l'identificazione avviene nel rispetto dei seguenti requisiti:

   a) Il certificato deve essere rilasciato da un certificatore accreditato dall'Agenzia per l'Italia Digitale ai sensi dell'art 29 del CAD, 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 token USB, secondo quanto previsto dalla normativa vigente. I dispositivi sicuri devono essere certificati Common Criterio 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 partico-lare, 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 tramite token crittografico, 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 ispet-tive, 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 ri-spetto dei requisiti.

5. L'identificazione informatica per i soggetti abilitati interni avviene ai sensi dell'articolo 10.

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 i 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 appartengo-no 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 im-prese, l'indice nazionale delle imprese e dei professionisti (INI-PEC), l'ana-grafe nazionale della popolazione residente (ANPR) e il domicilio digitale del cittadino di cui all'art 3-bis del CAD - sono recuperati gli indirizzi di PEC dei professionisti e delle imprese, nonché gli indirizzi dei cittadini ivi censi-ti.

6. Il ReGIndE è direttamente accessibile dai sistemi interni al dominio giusti-zia, 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, su connessioni sicure (SSL v3), attraverso un apposito web service; i relativi 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.do@giustiziacert.it.

3. Terminate le operazioni di censimento da parte del responsabile per i si-stemi informativi automatizzati, l'ente mittente del documento di censimen-to 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 consi-derati i messaggi di posta ordinaria;

   b) non vi sono vincoli sull'oggetto né sul corpo 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 o, per le Pubbliche Amministrazioni, ComunicazioneSoggettiPPAA.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 o il file ComunicazioneSoggettiPP.AA.xml deve essere conforme all'XML-Schema di cui all'Allegato 2;

g) il codice ente specificato nel file deve essere tra quelli censiti.

4. Il mancato rispetto di uno o più dei vincoli di cui all'articolo precedente comporta un messaggio automatico di esito negativo; in questo caso l'allegato ComunicazioniSoggetti.xml viene scartato.

5. A ogni invio corrisponde una risposta tramite PEC; il messaggio ha come oggetto la medesima descrizione del messaggio originale con il suffisso "Esito" e riporta in allegato l'esito dell'elaborazione del messaggio con le eventuali eccezioni; il formato del messaggio di esito, inviato come allegato al messaggio di PEC, è descritto nell'Allegato 3.

6. L'esito si riferisce sia ad errori presenti sui dati e, quindi riconducibili alle informazioni dei singoli soggetti (come ad esempio codice fiscale inesisten-te), 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, ef-fettuando altresì l'inserimento (upload) del file che contiene copia informa-tica, 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 pri-ma iscrizione e invia un messaggio PEC di cortesia al professionista.

ART. 9 bis

(Indirizzi di posta elettronica certificata delle pubbliche amministrazioni)

1. La pubblica amministrazione che deve comunicare il proprio indirizzo di posta elettronica certificata per la ricezione delle comunicazioni e notificazioni, ai sensi dell'articolo 16, comma 12, del decreto-legge 18 ottobre 2012, n. 179, convertito con modificazioni nella legge 17 dicembre 2012, n. 221, procede inserendo tale indirizzo sul portale dei servizi telematici.

2. Ai fini di cui al comma precedente, la pubblica amministrazione invia all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati (prot.dgsia.dog@giustiziacert.it) un documento contenente le seguenti informazioni:

   a) descrizione e codice fiscale della pubblica amministrazione;

   b) nominativo, codice fiscale e recapiti del soggetto incaricato di inserire o modificare gli indirizzi di PEC della pubblica amministrazione sul porta-le dei servizi telematici;

3. Il soggetto incaricato di cui al comma precedente accede ad un'apposita area riservata del portale dei servizi telematici, previa identificazione informatica, secondo le specifiche di cui all'articolo 6, e inserisce o modifica:

   a) l'indirizzo di PEC della pubblica amministrazione;

   b) il nominativo, il codice fiscale e l'indirizzo di PEC di eventuali dipendenti tramite i quali la pubblica amministrazione sta in giudizio personalmen-te; tali soggetti alimentano il Registro Generale degli Indirizzi Elettroni-ci.

4. L'elenco degli indirizzi di PEC delle pubbliche amministrazioni è consultabile dagli uffici giudiziari e dagli uffici NEP attraverso i sistemi informatici a disposizione dei soggetti abilitati interni.

5. L'elenco degli indirizzi di PEC di cui al comma 3, lettera a, è consultabile dagli avvocati 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, che verifica la presenza dell'avvocato sul ReGIndE; i relativi WSDL sono pubblicati nell'area pubblica del portale dei servizi telematici. L'accesso è tracciato in appositi log, che il Ministero della giustizia conserva per cinque anni, recanti: il punto di accesso attraverso cui è stato effettuato l'accesso, la data e l'ora dell'accesso.

ART. 10

(Sistemi informatici per i soggetti abilitati interni - art. 8 del regolamento)

1. I sistemi informatici a disposizione dei soggetti abilitati interni sono con-formi 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" oppure mediante autenticazione a due fattori.

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) tramite autenticazione a due fattori; 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) tutti i metodi - esposti attraverso appositi web service - necessari per il recupero, l'archiviazione e la conservazione dei documenti informatici, secondo la normativa 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, da depositare telematicamente all'ufficio giudiziario, rispetta i seguenti requisiti:

   f) è in formato PDF;

   g) è privo di elementi attivi;

   h) 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;

   i) è sottoscritto con firma digitale o firma elettronica qualificata esterna secondo la struttura riportata ai commi seguenti;

   j) 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 PAdES-BES (o PAdES Part 3) o CAdES-BES; il certificato di firma è inserito nella busta crittografica; è fatto divieto di inserire nella busta crittografica le informazioni di revoca riguardanti il certificato del firmatario. 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; nel caso del formato CAdES 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.

3. Le applicazioni di generazione della firma digitale o qualificata per la sottoscrizione dei documenti informatici devono utilizzare la funzione di hash di cui all'art 4, comma 2, del Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013

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) .rtf

   c) .txt

   d) .jpg

   e) .gif

   f) .tiff

   g) .xml

   h) .eml, purché contenenti file nei formati di cui alle lettere precedenti.

   i) .msg, purché contenenti file nei formati di cui alle lettere da a ad h.

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 sottoscritti 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. Tale file deve essere omesso qualora il suo contenuto sia presente nella sezione apposita del file DatiAtto.xml, come da XSD di cui al successivo punto b).

   b) DatiAtto.xml: gli XSD sono riportati nell'Allegato 5.

   c) <nome file (libero)>: atto vero e proprio, in formato PDF, sottoscritto con firma digitale o firma elettronica qualificata secondo la struttura dell'articolo 12 comma 2.

   d) AllegatoX.xxx: 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).

3. La dimensione massima consentita per la busta telematica è pari a 30 Megabyte.

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 (WARNING): 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)

I soggetti abilitati interni utilizzano appositi strumenti per la redazione degli atti del processo in forma di documento informatico e per la loro tra-smissione alla cancelleria o alla segreteria dell'ufficio giudiziario.

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.

Se il provvedimento del magistrato è in formato cartaceo, il cancelliere o il segretario dell'ufficio giudiziario ne estrae copia per immagine in formato PDF, e lo sottoscrive con firma digitale o firma elettronica qualificata.

ART. 17

(Comunicazioni e notificazioni per via telematica - art. 16 del regolamento)

1. Il gestore dei servizi telematici provvede ad inviare le comunicazioni o le notificazioni per via telematica, provenienti dall'ufficio giudiziario, alla casella di posta elettronica certificata del soggetto abilitato esterno o dell'utente privato destinatario, recuperando il relativo indirizzo dai pubblici elenchi ai sensi dell'art 16-ter del decreto legge del 30 ottobre 2012, n. 179 oppure ai sensi dell'art 16 comma 7 del medesimo decreto; il formato del messaggio è riportato nell'Allegato 8; la comunicazione o notificazione 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 per immagine in formato PDF di eventuali documenti cartacei da comunicare; la copia informatica è conservata nel fascicolo informatico.

3. Il gestore dei servizi telematici recupera le ricevute della posta elettronica certificata e gli avvisi di mancata consegna dal gestore di PEC del Ministero e li conserva nel fascicolo informatico; la ricevuta di avvenuta consegna è di tipo breve per le comunicazioni e di tipo completo per le notificazioni.

ART. 18

(Comunicazioni e notificazioni contenenti dati sensibili - art. 16 del regolamento)

1. La comunicazione o la notificazione che contiene dati sensibili è effettuata per estratto: in questo caso al destinatario viene recapitato l'avviso di disponibilità, 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 consultazione;

    b) il riferimento al documento prelevato o consultato (codice univoco inserito nell'URL inviato nell'avviso di cui al comma 4);

    c) la data e l'ora di invio dell'avviso;

    d) la data e l'ora del prelievo o della consultazione.

4. Le informazioni di cui al comma precedente vengono conservate per cinque anni.

5. Nel caso in cui il destinatario sia un'impresa iscritta nel relativo registro o una Pubblica Amministrazione, la comunicazione o la notificazione che contiene dati sensibili è effettuata ai sensi del comma 1; l'utente che accede all'indirizzo (URL) contenuto nel messaggio di PEC di avviso, su canale sicuro (protocollo SSL),

viene identificato ai sensi dell'art 6 ed è abilitato ad accedere all'atto integrale solo se appartiene all'impresa destinataria come risultante dal registro delle imprese o se è un dipendente della Pubblica Amministrazione autorizzato.

ART. 19

(Notificazioni per via telematica a cura degli uffici NEP - art. 17 del regolamento)

1. 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), oppure tramite posta elettronica certificata.

2. Le richieste di notifica effettuate dai soggetti abilitati esterni sono inoltrate all'UNEP tramite posta elettronica certificata, nel rispetto dei requisiti tec-nici di cui agli articoli 12, 13 e 14; all'interno della busta telematica è inse-rito 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 de-gli indirizzi elettronici, ai sensi dell'articolo 7, comma 6, nonché dall'in-dice nazionale delle imprese e dei professionisti (INI-PEC), sezione professionisti;

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 certifi-cata; il formato del messaggio è riportato nell'Allegato 7.

ART. 19 bis

(Notificazioni per via telematica eseguite dagli avvocati - art. 18 del regolamento)

1. Qualora l'atto da notificarsi sia un documento originale informatico, esso deve essere in formato PDF e ottenuto da una trasformazione di un documento testuale, senza restrizioni per le operazioni di selezione e copia di parti; non è ammessa la scansione di immagini. Il documento informatico così ottenuto è allegato al messaggio di posta elettronica certificata.

2. Nei casi diversi dal comma 1, i documenti informatici o copie informatiche, anche per immagine, di documenti analogici, allegati al messaggio di posta elettronica certificata, sono privi di elementi attivi, tra cui macro e campi variabili, e sono consentiti in formato PDF.

3. Nei casi in cui l'atto da notificarsi sia l'atto del processo da trasmettere telematicamente all'ufficio giudiziario (esempio: atto di citazione), si procede ai sensi del precedente comma 1.

4. Qualora il documento informatico, di cui ai commi precedenti, sia sottoscritto con firma digitale o firma elettronica qualificata, si applica quanto previsto all'articolo 12, comma 2.

5. La trasmissione in via telematica all'ufficio giudiziario delle ricevute previ-ste dall'articolo 3-bis, comma 3, della legge 21 gennaio 1994, n. 53, nonché della copia dell'atto notificato ai sensi dell'articolo 9, comma 1, della medesima legge, è effettuata inserendo l'atto notificato all'interno della busta te-lematica di cui all'art 14 e, come allegati, la ricevuta di accettazione e la ricevuta di avvenuta consegna relativa ad ogni destinatario della notificazio-ne; i dati identificativi relativi alle ricevute sono inseriti nel file DatiAtto.xml di cui all'articolo 12, comma 1, lettera e.

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 sicu-ro 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 si-stema 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 un 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 della piattaforma di gestione documentale è dotata di apparati HSM dedicati.

8. La trasmissione telematica delle informazioni relative alle notizie di reato avviene tramite cooperazione applicativa tra il sistema di gestione informatizzata dei registri presso l'ufficio del pubblico ministero e il Sistema Informativo Interforze del Ministero dell'Interno, secondo le specifiche del Sistema Pubblico di Cooperazione (SPCoop), su canale cifrato attraverso l'uso di certificati server. Le informazioni contenute nella busta di e-Government prevista dalle specifiche SPCoop sono in formato XML.

ART. 21

(Requisiti della casella di PEC del soggetto abilitato esterno - art. 20 del regolamento)

1. La casella di posta elettronica certificata di un soggetto abilitato esterno deve disporre di uno spazio disco minimo pari a 1 Gigabyte.

ART. 22

(Richiesta delle copie di atti e documenti - art. 21 del regolamento)

1. Per la richiesta telematica di copie di atti e documenti relativi al procedimento è disponibile, sul punto di accesso e sul portale dei servizi telematici, un servizio sincrono attraverso il quale individuare i documenti di cui richiedere copia e, in seguito al perfezionamento del pagamento, inoltrare la richiesta effettiva della copia stessa.

2. Il soggetto che ne ha diritto può richiedere:

   a) copia semplice in formato digitale;

   b) copia semplice per l'avvocato non costituito in formato digitale;

   c) copia autentica in formato digitale;

   d) copia esecutiva in formato digitale;

   e) copia semplice in formato cartaceo;

   f) copia autentica in formato cartaceo;

   g) copia esecutiva in formato cartaceo.

3. I dati relativi alla richiesta sono inoltrati all'ufficio giudiziario attraverso l'invocazione di un apposito web service; al richiedente è restituito l'identificativo univoco della richiesta inoltrata. Tale identificativo univoco è associato all'intero flusso di gestione della richiesta e di rilascio della copia.

4. Nel caso in cui la copia non possa essere rilasciata il sistema, in maniera automatica, comunica al richiedente l'impossibilità di evadere la richiesta.

ART. 23

(Rilascio delle copie di atti e documenti - art. 21 del regolamento)

1. Il rilascio della copia informatica di atti e documenti viene eseguito secondo le specifiche di cui all'articolo 16 del regolamento e dell'art. 23-bis del CAD; la copia è inviata al richiedente in allegato ad un messaggio di posta elet-tronica 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.

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, localizza-to sul gestore dei servizi telematici, incaricato di esporre i servizi sottoforma di web servi ce (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 deve essere localizzata all'interno della intranet del PdA stesso e non deve essere accessibile direttamente dall'esterno.

4. I punti di accesso possono a loro volta esporre i web servi ce forniti dal ge-store 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 servi ce 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 su canale sicuro (protocollo SSL) 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 telemati-ci attribuiscono all'utente un ruolo di consultazione, a seconda del registro di cancelleria; eseguita tale operazione, viene trasmesso al proxy di cui al comma 2 il codice fiscale del soggetto che effettua l'accesso (nell'header http) e il ruolo di consultazione stesso (nel messaggio SOAP); il proxy tra-smette la richiesta al web servi ce del gestore dei servizi telematici.

8. In base al ruolo di consultazione di cui al comma precedente, il sistema fornisce le autorizzazioni all'accesso rispetto alle informazioni anagrafiche contenute nei sistemi di gestione dei registri o sulla base dell'atto di delega previsto dal regolamento.

9. In fase di richiesta di attivazione, il punto di accesso può adottare meccanismi di identificazione basati sulla gestione federata delle identità digitali (modello GFID), secondo le specifiche dell'Agenzia per l'Italia Digitale; in questo caso, il Direttore Generale S.I.A., valutata la soluzione proposta e opportunamente descritta nel piano

della sicurezza, approva il meccanismo di identificazione che soddisfa il livello di sicurezza richiesto.

10. Il punto di accesso può consentire l'accesso a soggetti delegati da un utente registrato (soggetto delegante), con le stesse modalità di cui ai commi 7, 8 e 9, purchè il soggetto delegante abbia predisposto un atto di delega, sottoscritto con firma digitale, che il punto di accesso conserva per cinque anni unitamente alla tracciatura di ogni accesso effettuato su delega; le informazioni e gli atti di cui sopra sono forniti su richiesta al Ministero della giustizia.

11. Fuori dai casi previsti ai commi 1 e 10, l'architettura dei servizi di consultazione prevede in via residuale che il punto di accesso o il portale dei ser-vizi telematici effettuino, a seguito dell'identificazione di cui al comma 7, un link diretto dalle proprie pagine alla pagina principale del sito web che ren-de disponibili i servizi su canale sicuro (HTTPS); in questo caso i dati iden-tificativi del soggetto vengono inseriti nell'header HTTP della richiesta.

12. I servizi di consultazione attivi sono elencati, per singolo ufficio, nel catalo-go dei servizi telematici, di cui all'articolo 5, comma 5.

13. 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.

14. 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 identificazio-ne 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;

k) descrizione dell'eventuale processo di delega di cui al comma 10 nonché delle modalità di conservazione dell'elenco dei soggetti delegati e delle eventuali revoche delle deleghe;

l) descrizione della modalità di verifica dell'effettiva funzionalità e adegua-tezza del sistema di sicurezza del punto di accesso.

15. Ai fini dell'iscrizione nel suddetto elenco, il responsabile per i sistemi informativi automatizzati verifica il piano della sicurezza di cui al comma precedente e può disporre apposite verifiche in loco, in particolare per accertare il rispetto delle prescrizioni di sicurezza riportate nel presente provvedimento.

16. 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.

17. Il punto di accesso si dota di una casella di posta elettronica certificata, che comunica al responsabile per i sistemi informativi automatizzati, da utilizzarsi per inviare e ricevere comunicazioni con il Ministero della giustizia.

18. Il punto di accesso fornisce al Ministero della giustizia, su richiesta, i dati di censimento sul ReGIndE di cui articolo 8 comma 1 per i casi di iscrizione dei professionisti non iscritti in albi di cui articolo 9 comma 1.

19. Il punto di accesso verifica l'effettiva funzionalità e adeguatezza del sistema di sicurezza almeno una volta l'anno e provvede ad inviare l'esito delle stes-se, unitamente ad eventuali variazioni nei contenuti del piano, all'indirizzo di posta elettronica certificata del responsabile per i sistemi informativi automatizzati: prot. olgsia. dogg.,giustiziacert.it.

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 registrazione del soggetto abilitato esterno o dell'utente privato, prelevando il codice fiscale dal token crittografico dell'utente; attraverso un'apposita masche-ra 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.

3. I dati di cui al comma precedente, unitamente alla data in cui è avvenuta la registrazione, sono archiviati e conservati per cinque 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, isti-tuito presso un tribunale (ai sensi del Capo II, sezione 1, delle disposizioni di attuazione del codice di procedura civile), al PdA viene presentata copia elettronica in formato PDF del provvedimento di iscrizione all'albo stesso da parte del comitato; tale copia è sottoscritta con firma digitale o firma elettronica qualificata dal soggetto che s'iscrive.

6. Il punto di accesso è tenuto a conservare i documenti informatici di cui ai commi precedenti, e a renderli disponibili, su richiesta, al Ministero della giustizia.

7. I punti di accesso trasmettono al Ministero della giustizia le informazioni relative ai propri utenti registrati secondo le modalità di cui all'allegato 11.

CAPO V — PAGAMENTI TELEMATICI

ART. 26

(Requisiti relativi al processo di pagamento telematico - art. 30 del regolamento)

1. Al fine di comunicare in via telematica all'ufficio giudiziario l'avvenuto pagamento delle spese, dei diritti e del contributo unificato, la ricevuta di versamento è inserita come allegato della busta telematica nel caso di inoltro via PEC, oppure è associata alla richiesta telematica nel caso di istanza gestita tramite un flusso sincrono.

2. 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 pagamento attraverso strumenti telematici e di ottenere la ricevuta di pagamento attraverso il medesimo canale telematico; l'accesso ai servizi di pagamento avviene previa identificazione informatica di cui all'articolo 6.

3. Le regole per l'esecuzione del pagamento, le modalità di interconnessione tra i sistemi nonché le modalità di rendicontazione e riconciliazione dei pagamenti rispettano le Linee Guida emanate dall'Agenzia per l'Italia Digitale ai sensi dell'art 5 del D. Leg.vo 7 marzo 2005, n. 82, modificato dal decreto legge del 30 ottobre 2012, n. 179.

4. Il portale dei servizi telematici si avvale dell'infrastruttura e della piattafor-ma tecnologica messa a disposizione dall'Agenzia per l'Italia Digitale, attra-verso il Sistema Pubblico di Connettività, (Nodo dei Pagamenti-SPC) allo scopo di garantire l'interconnessione e l'interoperabilità tra le Pubbliche Amministrazioni e i Prestatori di Servizi di Pagamento;

5. Il portale dei servizi telematici espone ai punti di accesso servizi web per l'esecuzione dei pagamenti telematici utilizzando le funzionalità messe a disposizione dal Nodo dei Pagamenti-SPC. 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.

6. I punti di accesso possono mettere a disposizione dei propri utenti il servizio di pagamento telematico, definendo opportuni accordi con uno o più prestatori di servizi di pagamento, nel rispetto di quanto indicato al comma 3.

7. Nei casi di cui al precedente comma, il punto di accesso è garante nei confronti del Ministero della Giustizia del rispetto delle Linee Guida di cui al comma 3, relativamente alle modalità di riversamento verso la banca tesoriera e alla rendicontazione; il punto di accesso rispetta quanto indicato nelle Linee Guida relativamente al flusso di rendicontazione nei confronti del Ministero della Giustizia.

8. Il processo di pagamento consente all'utente di scegliere tra diverse modali-tà di pagamento messe a sua disposizione da una molteplicità di prestatori di servizi di pagamento che aderiscono all'infrastruttura del Nodo dei pa-gamenti-SPC.

9. La ricevuta di pagamento 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. 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 partico-lare qualifica il versamento attraverso un identificativo univoco di cui al successivo comma 5;

   b) contiene i dati identificativi del soggetto che esegue il pagamento, contiene una parte riservata (Dati Specifici Riscossione) per inserire informazioni elaborabili automaticamente dai sistemi della Giustizia;

   c) viene predisposta dal soggetto che procede al pagamento ed inviata dal portale dei servizi telematici al Nodo dei Pagamenti-SPC;

2. La Ricevuta Telematica (RT) è restituita al soggetto che ha eseguito il pagamento 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 mes-sa a disposizione dell'Agenzia per l'Italia Digitale.

4. Al fine di qualificare in maniera univoca il pagamento all'interno del domi-nio giustizia, è definito l'identificativo univoco di pagamento (IUV) secon-do i formati previsti dalle Linee Guida emanate dall'Agenzia per l'Italia Digi-tale ai sensi dell'art 5 del D. Leg.vo 7 marzo 2005, n. 82, modificato dal de-creto legge del 30 ottobre 2012, n. 179.

5. Lo IUV (identificato con il nome CRS nell'ambito Giustizia) è generato esclusivamente dal portale dei servizi telematici attraverso l'invocazione di un web service di cui all'art 26, comma 5 e ha il seguente formato «check digit» «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. Lo IUV viene inserito nella struttura RPT (elemento identificativoUnivocoVersamento) e viene restituito invariato 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, attraverso l'identificativo univoco, che la ricevuta telematica non sia stato già utilizzata per altri servizi di pagamento e, in caso di esito positivo del controllo, la ricevuta viene marcata al fine di non permetterne il riutilizzo.

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 a registrare la RT nel sistema RRT contestualmente al rilascio della stessa al soggetto abilitato esterno richiedente; la registrazione si conclude con esito positivo solo se lo IUV presente nella RT è stato generato dal portale dei servizi telematici

3. Per la registrazione della RT nel al sistema RRT, il portale dei servizi telematici espone un apposito web service il cui WSDL è pubblicato nell'area pubblica del portale dei servizi telematici.

4. Il sistema RRT permette la gestione delle RT e dei relativi identificativi uni-voci di pagamento secondo le modalità indicate nell'articolo 27.

5. Le informazioni relative ai pagamenti contenute nel sistema di cui al com-ma 1 sono messe a disposizione, sulla base di specifica convenzione da sottoscriversi con il

Direttore Generale S.I.A., 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 telematica possono consultare sul portale dei servizi telematici, previa identificazione informatica di cui all'articolo 6, le informazioni relative ai pagamenti contenute nel sistema di cui al comma 1.

ART. 29

(Diritto di copia - art. 31 del regolamento)

1. Il sistema informatico del Ministero della giustizia comunica all'interessato l'importo da versare per i diritti di copia; tale importo è calcolato, sulla base delle vigenti disposizioni normative e regolamentari, in base alle indicazioni fornite dall'interessato al momento dell'individuazione dei documenti di cui richiedere copia. L'informazione è messa a disposizione dell'interessato attraverso il servizio di richiesta copie attivo sul punto di accesso e sul portale dei servizi telematici; unitamente all'importo dei diritti ed oneri viene comunicato all'interessato anche l'identificativo univoco associato al flusso di gestione della richiesta e rilascio della copia.

2. La richiesta di copia è soddisfatta solo dopo che è pervenuta la ricevuta telematica di pagamento 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'art. 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. A decorrere dalla comunicazione di cui al comma 1, il soggetto abilitato esterno utilizza unicamente il sistema di trasmissione della posta elettronica certificata, così come disciplinato nel presente provvedimento.

3. 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.

4. Le pubbliche amministrazioni comunicano il proprio indirizzo di posta elettronica certificata ai sensi dell'art. 9 bis del presente provvedimento entro il novantesimo giorno dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica italiana; le pubbliche amministrazioni possono comunicare detto indirizzo anche successivamente alla scadenza di detto termine; l'indirizzo sarà sero consultabile dagli uffici giudiziari a partire dal 91° giorno dalla pubblicazione del presente provvedimento sulla Gazzetta Ufficiale della Repubblica italiana

ART 31

(Efficacia)

1. Fatto salvo quanto indicato dall'art. 30 comma 4, il presente provvedimento acquista efficacia decorsi 15 giorni dalla sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana e sostituisce l'analogo provvedimento del 18 luglio 2011

Paragrafo – 5.3. DECRETO LEGISLATIVO 7 marzo 2005, n. 82 Codice dell'amministrazione digitale.

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76, 87 e 117, secondo comma, lettera r), della Costituzione;

Visto l'articolo 14 della legge 23 agosto 1988, n. 400, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri;

Visto l'articolo 10 della legge 29 luglio 2003, n. 229, recante interventi in materia di qualità della regolazione, riassetto normativo e codificazione - legge di semplificazione 2001;

Vista la legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;

Visto il decreto legislativo 12 febbraio 1993, n. 39, recante norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'articolo 2, comma 1, lettera mm), della legge 23 ottobre 1992, n. 421;

Visto il decreto legislativo 30 luglio 1999, n. 300, recante disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri;

Visto il testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (Testo A), di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

Visto il decreto legislativo 30 marzo 2001, n. 165, recante norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche;

Visto il decreto legislativo 23 gennaio 2002, n. 10, recante attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali;

Vista la legge 9 gennaio 2004, n. 4, recante disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici;

Visto il decreto legislativo 20 febbraio 2004, n. 52, recante attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA;

Vista la preliminare deliberazione del Consiglio dei Ministri, adottata nella riunione dell'11 novembre 2004;

Esperita la procedura di notifica alla Commissione europea di cui alla direttiva 98/34/CE del Parlamento europeo e del Consiglio, del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio, del 20 luglio 1998, attuata dalla legge 21 giugno 1986, n. 317, così come modificata dal decreto legislativo 23 novembre 2000, n. 427;

Acquisito il parere della Conferenza unificata, ai sensi dell'articolo 8, del decreto legislativo 28 agosto 1997, n. 281, espresso nella riunione del 13 gennaio 2005;

Sentito il Garante per la protezione dei dati personali;

Udito il parere del Consiglio di Stato, espresso dalla Sezione consultiva per gli atti normativi nell'adunanza del 7 febbraio 2005;

Acquisito il parere delle competenti Commissioni della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei Ministri, adottata nella riunione del 4 marzo 2005;

Sulla proposta del Ministro per l'innovazione e le tecnologie, di concerto con il Ministro per la funzione pubblica, con il Ministro dell'economia e delle finanze, con il Ministro dell'interno, con il Ministro della giustizia, con il Ministro delle attività produttive e con il Ministro delle comunicazioni;

Emana il seguente decreto legislativo:

Capo I

PRINCIPI GENERALI

Sezione I

Definizioni, finalità e ambito di applicazione

Art. 1. Definizioni

1. Ai fini del presente codice si intende per:

a) allineamento dei dati: il processo di coordinamento dei dati presenti in più archivi finalizzato alla verifica della corrispondenza delle informazioni in essi contenute;

b) autenticazione del documento informatico: la validazione del documento informatico attraverso l'associazione di dati informatici relativi all'autore o alle circostanze, anche temporali, della redazione;

c) carta d'identità elettronica: il documento d'identità munito di elementi per l'identificazione fisica del titolare rilasciato su supporto informatico dalle amministrazioni comunali con la prevalente finalità di dimostrare l'identità anagrafica del suo titolare;

d) carta nazionale dei servizi: il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni;

e) certificati elettronici: gli attestati elettronici che collegano all'identità del titolare i dati utilizzati per verificare le firme elettroniche;

f) certificato qualificato: il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciati da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;

g) certificatore: il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime;

h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico;

i) chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche;

i-bis) copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto;

i-ter) copia per immagine su supporto informatico di documento analogico: il documento informatico avente contenuto e forma identici a quelli del documento analogico da cui è tratto;

i-quater) copia informatica di documento informatico: il documento informatico avente contenuto identico a quello del documento da cui è tratto su supporto informatico con diversa sequenza di valori binari;

i-quinquies) duplicato informatico: il documento informatico ottenuto mediante la memorizzazione, sullo stesso dispositivo o su dispositivi diversi, della medesima sequenza di valori binari del documento originario;

l) dato a conoscibilità limitata: il dato la cui conoscibilità è riservata per legge o regolamento a specifici soggetti o categorie di soggetti;

m) dato delle pubbliche amministrazioni: il dato formato, o comunque trattato da una pubblica amministrazione;

n) dato pubblico: il dato conoscibile da chiunque;

n-bis) riutilizzo: uso del dato di cui all'articolo 2, comma 1, lettera e), del decreto legislativo 24 gennaio 2006, n. 36;

o) disponibilità: la possibilità di accedere ai dati senza restrizioni non riconducibili a esplicite norme di legge;

p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti;

p-bis) documento analogico: la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti;

q) firma elettronica: l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica;

q-bis) firma elettronica avanzata: insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati;

r) firma elettronica qualificata: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

s) firma digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici;

t) fruibilità di un dato: la possibilità di utilizzare il dato anche trasferendolo nei sistemi informativi automatizzati di un'altra amministrazione;

u) gestione informatica dei documenti: l'insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione,

assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell'ambito del sistema di classificazione d'archivio adottato, effettuate mediante sistemi informatici;

u-bis) gestore di posta elettronica certificata: il soggetto che presta servizi di trasmissione dei documenti informatici mediante la posta elettronica certificata;

u-ter) identificazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso;

v) originali non unici: i documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi;

v-bis) posta elettronica certificata: sistema di comunicazione in grado di attestare l'invio e l'avvenuta consegna di un messaggio di posta elettronica e di fornire ricevute opponibili ai terzi;

z) pubbliche amministrazioni centrali: le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300;

aa) titolare: la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica;

bb) validazione temporale: il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

Art. 2. Finalità e ambito di applicazione

1. Lo Stato, le Regioni e le autonomie locali assicurano la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale e si organizzano ed agiscono a tale fine utilizzando con le modalità più appropriate le tecnologie dell'informazione e della comunicazione.

2. Le disposizioni del presente codice si applicano alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, nonché alle società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione, come individuate dall'Istituto nazionale di statistica (ISTAT) ai sensi dell'articolo 1, comma 5, della legge 30 dicembre 2004, n. 311.

[2-bis. abrogato]

3. Le disposizioni di cui al capo II, agli articoli 40, 43 e 44 del capo III, nonché al capo IV, si applicano ai privati ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni.

4. Le disposizioni di cui al capo V, concernenti l'accesso ai documenti informatici, e la fruibilità delle informazioni digitali si applicano anche ai gestori di servizi pubblici ed agli organismi di diritto pubblico.

5. Le disposizioni del presente codice si applicano nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196. I cittadini e le imprese hanno, comunque, diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.

6. Le disposizioni del presente codice non si applicano limitatamente all'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, e consultazioni elettorali. Con decreti del Presidente del Consiglio dei Ministri, tenuto conto delle esigenze derivanti dalla natura delle proprie particolari funzioni, sono stabiliti le modalità, i limiti ed i tempi di applicazione delle disposizioni del presente Codice alla Presidenza del Consiglio dei Ministri, nonché all'Amministrazione economico-finanziaria.

Sezione II

Diritti dei cittadini e delle imprese

Art. 3. Diritto all'uso delle tecnologie

1. I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni, con i soggetti di cui all'articolo 2, comma 2, e con i gestori di pubblici servizi ai sensi di quanto previsto dal presente codice.

[1-bis. arogato]

1-ter. La tutela giurisdizionale davanti al giudice amministrativo è disciplinata dal codice del processo amministrativo.

Art. 3-bis Domicilio digitale del cittadino

1. l fine di facilitare la comunicazione tra pubbliche amministrazioni e cittadini, è facoltà di ogni cittadino indicare alla pubblica amministrazione, secondo le modalità stabilite al comma 3, un proprio indirizzo di posta elettronica certificata, rilasciato ai sensi

dell'articolo 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, quale suo domicilio digitale.

2. L'indirizzo di cui al comma 1 è inserito nell'Anagrafe nazionale della popolazione residente-ANPR e reso disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi.

3. Con decreto del Ministro dell'interno, di concerto con il Ministro per la pubblica amministrazione e la semplificazione e il Ministro delegato per l'innovazione tecnologica, sentita l'Agenzia per l'Italia digitale, sono definite le modalità di comunicazione, variazione e cancellazione del proprio domicilio digitale da parte del cittadino, nonché le modalità di consultazione dell'ANPR da parte dei gestori o esercenti di pubblici servizi ai fini del reperimento del domicilio digitale dei propri utenti.

4. A decorrere dal 1° gennaio 2013, salvo i casi in cui è prevista dalla normativa vigente una diversa modalità di comunicazione o di pubblicazione in via telematica, le amministrazioni pubbliche e i gestori o esercenti di pubblici servizi comunicano con il cittadino esclusivamente tramite il domicilio digitale dallo stesso dichiarato, anche ai sensi dell'articolo 21-bis della legge 7 agosto 1990, n. 241, senza oneri di spedizione a suo carico. Ogni altra forma di comunicazione non può produrre effetti pregiudizievoli per il destinatario. L'utilizzo di differenti modalità di comunicazione rientra tra i parametri di valutazione della performance dirigenziale ai sensi dell'articolo 11, comma 9, del decreto legislativo 27 ottobre 2009, n. 150.

4-bis. In assenza del domicilio digitale di cui al comma 1, le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata, da conservare nei propri archivi, ed inviare ai cittadini stessi, per posta ordinaria o raccomandata con avviso di ricevimento, copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del decreto legislativo 12 dicembre 1993, n. 39.

4-ter. Le disposizioni di cui al comma 4-bis soddisfano a tutti gli effetti di legge gli obblighi di conservazione e di esibizione dei documenti previsti dalla legislazione vigente laddove la copia analogica inviata al cittadino contenga una dicitura che specifichi che il documento informatico, da cui la copia è tratta, è stato predisposto e conservato presso l'amministrazione in conformità alle regole tecniche di cui all'articolo 71.

4-quater. Le modalità di predisposizione della copia analogica di cui ai commi 4-bis e 4-ter soddisfano le condizioni di cui all'articolo 23-ter, comma 5, salvo i casi in cui il documento rappresenti, per propria natura, una certificazione rilasciata dall'amministrazione da utilizzarsi nei rapporti tra privati.

5. Dall'attuazione delle disposizioni di cui al presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica.

Art. 4. Partecipazione al procedimento amministrativo informatico

1. La partecipazione al procedimento amministrativo e il diritto di accesso ai documenti amministrativi sono esercitabili mediante l'uso delle tecnologie dell'informazione e della comunicazione secondo quanto disposto dagli articoli 59 e 60 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

2. Ogni atto e documento può essere trasmesso alle pubbliche amministrazioni con l'uso delle tecnologie dell'informazione e della comunicazione se formato ed inviato nel rispetto della vigente normativa.

Art. 5. Effettuazione di pagamenti con modalità informatiche

1. I soggetti di cui all'articolo 2, comma 2, e i gestori di pubblici servizi nei rapporti con l'utenza sono tenuti a far data dal 1° giugno 2013 ad accettare i pagamenti ad essi spettanti, a qualsiasi titolo dovuti, anche con l'uso delle tecnologie dell'informazione e della comunicazione. A tal fine:

a) sono tenuti a pubblicare nei propri siti istituzionali e a specificare nelle richieste di pagamento:

1) i codici IBAN identificativi del conto di pagamento, ovvero dell'imputazione del versamento in Tesoreria, di cui all'articolo 3 del decreto del Ministro dell'economia e delle finanze 9 ottobre 2006, n. 293, tramite i quali i soggetti versanti possono effettuare i pagamenti mediante bonifico bancario o postale, ovvero gli identificativi del conto corrente postale sul quale i soggetti versanti possono effettuare i pagamenti mediante bollettino postale;

2) i codici identificativi del pagamento da indicare obbligatoriamente per il versamento;

b) si avvalgono di prestatori di servizi di pagamento, individuati mediante ricorso agli strumenti di acquisto e negoziazione messi a disposizione da Consip o dalle centrali di committenza regionali di riferimento costituite ai sensi dell'articolo 1, comma 455, della legge 27 dicembre 2006, n. 296, per consentire ai privati di effettuare i pagamenti in loro favore attraverso l'utilizzo di carte di debito, di credito, prepagate ovvero di altri strumenti di pagamento elettronico disponibili, che consentano anche l'addebito in conto corrente, indicando sempre le condizioni, anche economiche, per il loro utilizzo. Il prestatore dei servizi di pagamento, che riceve l'importo dell'operazione di pagamento, effettua il riversamento dell'importo trasferito al tesoriere dell'ente, registrando in apposito sistema informatico, a disposizione dell'amministrazione, il pagamento eseguito, i codici identificativi del pagamento medesimo, nonché i codici IBAN identificativi dell'utenza bancaria ovvero dell'imputazione del versamento in Tesoreria. Le modalità di movimentazione tra le sezioni di Tesoreria e Poste Italiane S.p.A. dei fondi connessi alle operazioni effettuate sui conti correnti postali intestati a pubbliche amministrazioni sono regolate dalla convenzione tra il Ministero dell'economia e delle finanze e Poste Italiane

S.p.A. stipulata ai sensi dell'articolo 2, comma 2, del decreto-legge 1° dicembre 1993, n. 487, convertito, con modificazioni, dalla legge 29 gennaio 1994, n. 71.

2. Per le finalità di cui al comma 1, lettera b), le amministrazioni e i soggetti di cui al comma 1 possono altresì avvalersi dei servizi erogati dalla piattaforma di cui all'articolo 81 comma 2-bis e dei prestatori di servizi di pagamento abilitati.

3. Dalle previsioni di cui alla lettera a) del comma 1 possono essere escluse le operazioni di pagamento per le quali la verifica del buon fine dello stesso debba essere contestuale all'erogazione del servizio; in questi casi devono comunque essere rese disponibili modalità di pagamento di cui alla lettera b) del medesimo comma 1.

3-bis. I micro-pagamenti dovuti a titolo di corrispettivo dalle pubbliche amministrazioni di cui all'articolo 1, comma 450, della legge 27 dicembre 2006, n. 296, come modificato dall'articolo 7, comma 2, del decreto-legge 7 maggio 2012, n. 52, convertito, con modificazioni, dalla legge 6 luglio 2012, n. 94, per i contratti di acquisto di beni e servizi conclusi tramite gli strumenti elettronici di cui al medesimo articolo 1, comma 450, stipulati nelle forme di cui all'articolo 11, comma 13, del codice di cui al decreto legislativo 12 aprile 2006, n. 163, e successive modificazioni, sono effettuati mediante strumenti elettronici di pagamento se richiesto dalle imprese fornitrici.

3-ter. Con decreto del Ministero dell'economia e delle finanze da pubblicare entro il 1° marzo 2013 sono definiti i micro-pagamenti in relazione al volume complessivo del contratto e sono adeguate alle finalità di cui al comma 3-bis le norme relative alle procedure di pagamento delle pubbliche amministrazioni di cui al citato articolo 1, comma 450, della legge n. 296 del 2006. Le medesime pubbliche amministrazioni provvedono ad adeguare le proprie norme al fine di consentire il pagamento elettronico per gli acquisti di cui al comma 3-bis entro il 1° gennaio 2013.

4. L'Agenzia per l'Italia digitale, sentita la Banca d'Italia, definisce linee guida per la specifica dei codici identificativi del pagamento di cui al comma 1, lettere a) e b) e le modalità attraverso le quali il prestatore dei servizi di pagamento mette a disposizione dell'ente le informazioni relative al pagamento medesimo. (32)

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

Art. 5-bis Comunicazioni tra imprese e amministrazioni pubbliche

1. La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese.

2. Con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro per la pubblica amministrazione e l'innovazione, di concerto con il Ministro dello sviluppo

economico e con il Ministro per la semplificazione normativa, sono adottate le modalità di attuazione del comma 1 da parte delle pubbliche amministrazioni centrali e fissati i relativi termini.

3. DigitPA, anche avvalendosi degli uffici di cui all'articolo 17, provvede alla verifica dell'attuazione del comma 1 secondo le modalità e i termini indicati nel decreto di cui al comma 2.

4. Il Governo promuove l'intesa con regioni ed enti locali in sede di Conferenza unificata per l'adozione degli indirizzi utili alla realizzazione delle finalità di cui al comma 1.

Art. 6. Utilizzo della posta elettronica certificata

1. Per le comunicazioni di cui all'articolo 48, comma 1, con i soggetti che hanno preventivamente dichiarato il proprio indirizzo ai sensi della vigente normativa tecnica, le pubbliche amministrazioni utilizzano la posta elettronica certificata. La dichiarazione dell'indirizzo vincola solo il dichiarante e rappresenta espressa accettazione dell'invio, tramite posta elettronica certificata, da parte delle pubbliche amministrazioni, degli atti e dei provvedimenti che lo riguardano.

1-bis. La consultazione degli indirizzi di posta elettronica certificata, di cui agli articoli 16, comma 10, e 16-bis, comma 5, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, e l'estrazione di elenchi dei suddetti indirizzi, da parte delle pubbliche amministrazioni è effettuata sulla base delle regole tecniche emanate da DigitPA, sentito il Garante per la protezione dei dati personali. (37)

[2. abrogato]

[2-bis. abrogato]

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

1. Al fine di favorire la presentazione di istanze, dichiarazioni e dati, nonché lo scambio di informazioni e documenti tra la pubblica amministrazione e le imprese e i professionisti in modalità telematica, è istituito, entro sei mesi dalla data di entrata in vigore della presente disposizione e con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente, il pubblico elenco denominato Indice nazionale degli indirizzi di posta elettronica certificata (INI-PEC) delle imprese e dei professionisti, presso il Ministero per lo sviluppo economico.

2. L'Indice nazionale di cui al comma 1 è realizzato a partire dagli elenchi di indirizzi PEC costituiti presso il registro delle imprese e gli ordini o collegi professionali, in attuazione di quanto previsto dall'articolo 16 del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2.

3. L'accesso all'INI-PEC è consentito alle pubbliche amministrazioni, ai professionisti, alle imprese, ai gestori o esercenti di pubblici servizi ed a tutti i cittadini tramite sito web e senza necessità di autenticazione. L'indice è realizzato in formato aperto, secondo la definizione di cui all'articolo 68, comma 3.

4. Il Ministero per lo sviluppo economico, al fine del contenimento dei costi e dell'utilizzo razionale delle risorse, sentita l'Agenzia per l'Italia digitale, si avvale per la realizzazione e gestione operativa dell'Indice nazionale di cui al comma 1 delle strutture informatiche delle Camere di commercio deputate alla gestione del registro imprese e ne definisce con proprio decreto, da emanare entro 60 giorni dalla data di entrata in vigore della presente disposizione, le modalità di accesso e di aggiornamento.

5. Nel decreto di cui al comma 4 sono anche definite le modalità e le forme con cui gli ordini e i collegi professionali comunicano all'Indice nazionale di cui al comma 1 tutti gli indirizzi PEC relativi ai professionisti di propria competenza e sono previsti gli strumenti telematici resi disponibili dalle Camere di commercio per il tramite delle proprie strutture informatiche al fine di ottimizzare la raccolta e aggiornamento dei medesimi indirizzi.

6. Dall'attuazione delle disposizioni di cui al presente articolo non devono derivare nuovi o maggiori oneri a carico della finanza pubblica.

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

1. Le pubbliche amministrazioni provvedono alla riorganizzazione ed aggiornamento dei servizi resi; a tale fine sviluppano l'uso delle tecnologie dell'informazione e della comunicazione, sulla base di una preventiva analisi delle reali esigenze dei cittadini e delle imprese, anche utilizzando strumenti per la valutazione del grado di soddisfazione degli utenti.

2. Entro il 31 maggio di ciascun anno le pubbliche amministrazioni centrali trasmettono al Ministro delegato per la funzione pubblica e al Ministro delegato per l'innovazione e le tecnologie una relazione sulla qualità dei servizi resi e sulla soddisfazione dell'utenza.

Art. 8. Alfabetizzazione informatica dei cittadini

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

Art. 9. Partecipazione democratica elettronica

1. Le pubbliche amministrazioni favoriscono ogni forma di uso delle nuove tecnologie per promuovere una maggiore partecipazione dei cittadini, anche residenti all'estero, al

processo democratico e per facilitare l'esercizio dei diritti politici e civili sia individuali che collettivi.

Art. 10. Sportello unico per le attività produttive

1. Lo sportello unico per le attività produttive di cui all'articolo 38, comma 3, del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133, eroga i propri servizi verso l'utenza in via telematica.

[2. abrogato]

[3. abrogato]

4. Lo Stato realizza, nell'ambito di quanto previsto dal sistema pubblico di connettività di cui al presente decreto, un sistema informatizzato per le imprese relativo ai procedimenti di competenza delle amministrazioni centrali anche ai fini di quanto previsto all'articolo 11.

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

1. Presso il Ministero delle attività produttive, che si avvale a questo scopo del sistema informativo delle camere di commercio, industria, artigianato e agricoltura, è istituito il Registro informatico degli adempimenti amministrativi per le imprese, di seguito denominato «Registro», il quale contiene l'elenco completo degli adempimenti amministrativi previsti dalle pubbliche amministrazioni per l'avvio e l'esercizio delle attività di impresa, nonché i dati raccolti dalle amministrazioni comunali negli archivi informatici di cui all'articolo 24, comma 2, del decreto legislativo 31 marzo 1998, n. 112. Il Registro, che si articola su base regionale con apposite sezioni del sito informatico, fornisce, ove possibile, il supporto necessario a compilare in via elettronica la relativa modulistica.

2. E' fatto obbligo alle amministrazioni pubbliche, nonché ai concessionari di lavori e ai concessionari e gestori di servizi pubblici, di trasmettere in via informatica al Ministero delle attività produttive l'elenco degli adempimenti amministrativi necessari per l'avvio e l'esercizio dell'attività di impresa.

3. Con decreto del Presidente del Consiglio dei Ministri, su proposta del Ministro delle attività produttive e del Ministro delegato per l'innovazione e le tecnologie, sono stabilite le modalità di coordinamento, di attuazione e di accesso al Registro, nonché di connessione informatica tra le diverse sezioni del sito.

4. Il Registro è pubblicato su uno o più siti telematici, individuati con decreto del Ministro delle attività produttive.

5. Del Registro possono avvalersi le autonomie locali, qualora non provvedano in proprio, per i servizi pubblici da loro gestiti.

6. All'onere derivante dall'attuazione del presente articolo si provvede ai sensi dell'articolo 21, comma 2, della legge 29 luglio 2003, n. 229.

Sezione III

Organizzazione delle pubbliche amministrazioni

Rapporti fra Stato, Regioni e autonomie locali

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

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

1-bis. Gli organi di Governo nell'esercizio delle funzioni di indirizzo politico ed in particolare nell'emanazione delle direttive generali per l'attività amministrativa e per la gestione ai sensi del comma 1 dell'articolo 14 del decreto legislativo 30 marzo 2001, n. 165, e le amministrazioni pubbliche nella redazione del piano di performance di cui all'articolo 10 del decreto legislativo 27 ottobre 2009, n. 150, dettano disposizioni per l'attuazione delle disposizioni del presente decreto.

1-ter. I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al presente decreto ai sensi e nei limiti degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165, ferme restando le eventuali responsabilità penali, civili e contabili previste dalle norme vigenti. L'attuazione delle disposizioni del presente decreto è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti.

2. Le pubbliche amministrazioni adottano le tecnologie dell'informazione e della comunicazione nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati, con misure informatiche, tecnologiche e procedurali di sicurezza, secondo le regole tecniche di cui all'articolo 71.

3. Le pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici, ivi comprese le reti di telefonia fissa e mobile in tutte le loro articolazioni, da esse erogati, qualunque sia il canale di erogazione, nel rispetto della autonomia e della specificità di ciascun erogatore di servizi.

4. Lo Stato promuove la realizzazione e l'utilizzo di reti telematiche come strumento di interazione tra le pubbliche amministrazioni ed i privati.

5. Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo, nel rispetto delle vigenti normative, l'accesso alla consultazione, la circolazione e lo scambio di dati e informazioni, nonché l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

5-bis. Le pubbliche amministrazioni implementano e consolidano i processi di informatizzazione in atto, ivi compresi quelli riguardanti l'erogazione attraverso le tecnologie dell'informazione e della comunicazione in via telematica di servizi a cittadini ed imprese anche con l'intervento di privati.

Art. 13. Formazione informatica dei dipendenti pubblici

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

Art. 14. Rapporti tra Stato, Regioni e autonomie locali

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

2. Lo Stato, le regioni e le autonomie locali promuovono le intese e gli accordi e adottano, attraverso la Conferenza unificata, gli indirizzi utili per realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso e per l'individuazione delle regole tecniche di cui all'articolo 71.

2-bis. Le regioni promuovono sul territorio azioni tese a realizzare un processo di digitalizzazione dell'azione amministrativa coordinato e condiviso tra le autonomie locali.

2-ter. Le regioni e gli enti locali digitalizzano la loro azione amministrativa e implementano l'utilizzo delle tecnologie dell'informazione e della comunicazione per garantire servizi migliori ai cittadini e alle imprese. (56)

3. Lo Stato, ai fini di quanto previsto ai commi 1 e 2, istituisce organismi di cooperazione con le regioni e le autonomie locali, promuove intese ed accordi tematici e territoriali, favorisce la collaborazione interregionale, incentiva la realizzazione di progetti a livello locale, in particolare mediante il trasferimento delle soluzioni tecniche ed organizzative, previene il divario tecnologico tra amministrazioni di diversa dimensione e collocazione territoriale.

3-bis. Ai fini di quanto previsto ai commi 1, 2 e 3, è istituita senza nuovi o maggiori oneri per la finanza pubblica, presso la Conferenza unificata, previa delibera della medesima che ne definisce la composizione e le specifiche competenze, una Commissione permanente per l'innovazione tecnologica nelle regioni e negli enti locali con funzioni istruttorie e consultive.

Art. 15. Digitalizzazione e riorganizzazione

1. La riorganizzazione strutturale e gestionale delle pubbliche amministrazioni volta al perseguimento degli obiettivi di cui all'articolo 12, comma 1, avviene anche attraverso il migliore e più esteso utilizzo delle tecnologie dell'informazione e della comunicazione nell'ambito di una coordinata strategia che garantisca il coerente sviluppo del processo di digitalizzazione.

2. In attuazione del comma 1, le pubbliche amministrazioni provvedono in particolare a razionalizzare e semplificare i procedimenti amministrativi, le attività gestionali, i documenti, la modulistica, le modalità di accesso e di presentazione delle istanze da parte dei cittadini e delle imprese, assicurando che l'utilizzo delle tecnologie dell'informazione e della comunicazione avvenga in conformità alle prescrizioni tecnologiche definite nelle regole tecniche di cui all'articolo 71.

2-bis. Le pubbliche amministrazioni nella valutazione dei progetti di investimento in materia di innovazione tecnologica tengono conto degli effettivi risparmi derivanti dalla razionalizzazione di cui al comma 2, nonché dei costi e delle economie che ne derivano.

2-ter. Le pubbliche amministrazioni, quantificano annualmente, ai sensi dell'articolo 27, del decreto legislativo 27 ottobre 2009, n. 150, i risparmi effettivamente conseguiti in attuazione delle disposizioni di cui ai commi 1 e 2. Tali risparmi sono utilizzati, per due terzi secondo quanto previsto dall'articolo 27, comma 1, del citato decreto legislativo n. 150 del 2009 e in misura pari ad un terzo per il finanziamento di ulteriori progetti di innovazione.

3. La digitalizzazione dell'azione amministrativa è attuata dalle pubbliche amministrazioni con modalità idonee a garantire la partecipazione dell'Italia alla costruzione di reti transeuropee per lo scambio elettronico di dati e servizi fra le amministrazioni dei Paesi membri dell'Unione europea.

[3-bis. abrogato]

[3-ter. abrogato]

[3-quater. abrogato]

[3-quinquies. abrogato]

[3-sexies. abrogato]

[3-septies. abrogato]

[3-octies. abrogato]

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

1. Per il perseguimento dei fini di cui al presente codice, il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie, nell'attività di coordinamento del processo di digitalizzazione e di coordinamento e di valutazione dei programmi, dei progetti e dei piani di azione formulati dalle pubbliche amministrazioni centrali per lo sviluppo dei sistemi informativi:

a) definisce con proprie direttive le linee strategiche, la pianificazione e le aree di intervento dell'innovazione tecnologica nelle pubbliche amministrazioni centrali, e ne verifica l'attuazione;

b) valuta, sulla base di criteri e metodiche di ottimizzazione della spesa, il corretto utilizzo delle risorse finanziarie per l'informatica e la telematica da parte delle singole amministrazioni centrali;

c) sostiene progetti di grande contenuto innovativo, di rilevanza strategica, di preminente interesse nazionale, con particolare attenzione per i progetti di carattere intersettoriale;

d) promuove l'informazione circa le iniziative per la diffusione delle nuove tecnologie;

e) detta norme tecniche ai sensi dell'articolo 71 e criteri in tema di pianificazione, progettazione, realizzazione, gestione, mantenimento dei sistemi informativi automatizzati delle pubbliche amministrazioni centrali e delle loro interconnessioni, nonché della loro qualità e relativi aspetti organizzativi e della loro sicurezza.

2. Il Presidente del Consiglio dei Ministri o il Ministro delegato per l'innovazione e le tecnologie riferisce annualmente al Parlamento sullo stato di attuazione del presente codice.

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

1. Le pubbliche amministrazioni centrali garantiscono l'attuazione delle linee strategiche per la riorganizzazione e digitalizzazione dell'amministrazione definite dal Governo. A tale fine, le predette amministrazioni individuano un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, responsabile del coordinamento funzionale. Al predetto ufficio afferiscono i compiti relativi a:

a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;

b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;

c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;

d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;

e) analisi della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;

f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);

g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;

h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a cittadini e imprese mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;

i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;

j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di posta elettronica, protocollo informatico, firma digitale e mandato informatico, e delle norme in materia di accessibilità e fruibilità.

1-bis. Per lo svolgimento dei compiti di cui al comma 1, le Agenzie, le Forze armate, compresa l'Arma dei carabinieri e il Corpo delle capitanerie di porto, nonché i Corpi di polizia hanno facoltà di individuare propri uffici senza incrementare il numero complessivo di quelli già previsti nei rispettivi assetti organizzativi. (62)

1-ter. DigitPA assicura il coordinamento delle iniziative di cui al comma 1, lettera c), con le modalità di cui all'articolo 51.

Art. 18. Conferenza permanente per l'innovazione tecnologica

1. E' istituita la Conferenza permanente per l'innovazione tecnologica con funzioni di consulenza al Presidente del Consiglio dei Ministri, o al Ministro delegato per l'innovazione e le tecnologie, in materia di sviluppo ed attuazione dell'innovazione tecnologica nelle amministrazioni dello Stato.

2. La Conferenza permanente per l'innovazione tecnologica è presieduta da un rappresentante della Presidenza del Consiglio dei Ministri designato dal Presidente del

Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie; ne fanno parte il Presidente di DigitPA, i componenti di DigitPA, il Capo del Dipartimento per l'innovazione e le tecnologie, nonché i responsabili delle funzioni di cui all'articolo 17.

3. La Conferenza permanente per l'innovazione tecnologica si riunisce con cadenza almeno semestrale per la verifica dello stato di attuazione dei programmi in materia di innovazione tecnologica e del piano triennale di cui all'articolo 9 del decreto legislativo 12 febbraio 1993, n. 39.

4. Il Presidente del Consiglio dei Ministri, o il Ministro delegato per l'innovazione e le tecnologie, provvede, con proprio decreto, a disciplinare il funzionamento della Conferenza permanente per l'innovazione tecnologica.

5. La Conferenza permanente per l'innovazione tecnologica può sentire le organizzazioni produttive e di categoria.

6. La Conferenza permanente per l'innovazione tecnologica opera senza rimborsi spese o compensi per i partecipanti a qualsiasi titolo dovuti, compreso il trattamento economico di missione; dal presente articolo non devono derivare nuovi o maggiori oneri per il bilancio dello Stato.

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

1. E' istituita presso la Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, una banca dati contenente la normativa generale e speciale in materia di rapporto di lavoro alle dipendenze delle pubbliche amministrazioni.

2. La Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica, cura l'aggiornamento periodico della banca dati di cui al comma 1, tenendo conto delle innovazioni normative e della contrattazione collettiva successivamente intervenuta, e assicurando agli utenti la consultazione gratuita.

3. All'onere derivante dall'attuazione del presente articolo si provvede ai sensi dell'articolo 21, comma 3, della legge 29 luglio 2003, n. 229.

Capo II

DOCUMENTO INFORMATICO E FIRME ELETTRONICHE; TRASFERIMENTI DI FONDI, LIBRI E SCRITTURE

Sezione I

Documento informatico

Art. 20. Documento informatico

1. Il documento informatico da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui

all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice.

1-bis. L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità, fermo restando quanto disposto dall'articolo 21.

[2. abrogato]

3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, sono stabilite ai sensi dell'articolo 71. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

4. Con le medesime regole tecniche sono definite le misure tecniche, organizzative e gestionali volte a garantire l'integrità, la disponibilità e la riservatezza delle informazioni contenute nel documento informatico.

5. Restano ferme le disposizioni di legge in materia di protezione dei dati personali.

5-bis. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71.

Art. 21. Documento informatico sottoscritto con firma elettronica

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità.

2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.

2-bis. Salvo quanto previsto dall'articolo 25, le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12, del codice civile, se fatte con documento informatico, sono sottoscritte, a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13), del codice civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale.

3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate.

4. Le disposizioni del presente articolo si applicano anche se la firma elettronica è basata su un certificato qualificato rilasciato da un certificatore stabilito in uno Stato non facente parte dell'Unione europea, quando ricorre una delle seguenti condizioni:

a) il certificatore possiede i requisiti di cui alla direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, ed è accreditato in uno Stato membro;

b) il certificato qualificato è garantito da un certificatore stabilito nella Unione europea, in possesso dei requisiti di cui alla medesima direttiva;

c) il certificato qualificato, o il certificatore, è riconosciuto in forza di un accordo bilaterale o multilaterale tra l'Unione europea e Paesi terzi o organizzazioni internazionali.

5. Gli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto sono assolti secondo le modalità definite con uno o più decreti del Ministro dell'economia e delle finanze, sentito il Ministro delegato per l'innovazione e le tecnologie.

Art. 22. Copie informatiche di documenti analogici

1. I documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata. La loro esibizione e produzione sostituisce quella dell'originale.

2. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71.

3. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

4. Le copie formate ai sensi dei commi 1, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.

5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

6. Fino alla data di emanazione del decreto di cui al comma 5 per tutti i documenti analogici originali unici permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

Art. 23. Copie analogiche di documenti informatici

1. Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

2. Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico.

Art. 23-bis Duplicati e copie informatiche di documenti informatici

1. I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti, se prodotti in conformità alle regole tecniche di cui all'articolo 71.

2. Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

Art. 23-ter Documenti amministrativi informatici

1. Gli atti formati dalle pubbliche amministrazioni con strumenti informatici, nonché i dati e i documenti informatici detenuti dalle stesse, costituiscono informazione primaria

ed originale da cui è possibile effettuare, su diversi o identici tipi di supporto, duplicazioni e copie per gli usi consentiti dalla legge.

2. I documenti costituenti atti amministrativi con rilevanza interna al procedimento amministrativo sottoscritti con firma elettronica avanzata hanno l'efficacia prevista dall'art. 2702 del codice civile.

3. Le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71; in tale caso l'obbligo di conservazione dell'originale del documento è soddisfatto con la conservazione della copia su supporto informatico.

4. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il Ministro per i beni e le attività culturali, nonché d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e sentiti DigitPA e il Garante per la protezione dei dati personali.

5. Sulle copie analogiche di documenti amministrativi informatici può essere apposto a stampa un contrassegno, sulla base dei criteri definiti con linee guida dell'Agenzia per l'Italia digitale, tramite il quale è possibile ottenere il documento informatico, ovvero verificare la corrispondenza allo stesso della copia analogica. Il contrassegno apposto ai sensi del primo periodo sostituisce a tutti gli effetti di legge la sottoscrizione autografa e non può essere richiesta la produzione di altra copia analogica con sottoscrizione autografa del medesimo documento informatico. I programmi software eventualmente necessari alla verifica sono di libera e gratuita disponibilità.

5-bis. I documenti di cui al presente articolo devono essere fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all'articolo 11 della legge 9 gennaio 2004, n. 4.

6. Per quanto non previsto dal presente articolo si applicano gli articoli 21, 22, 23 e 23-bis.

Art. 23-quater Riproduzioni informatiche

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

Sezione II

Firme elettroniche e certificatori

Art. 24. Firma digitale

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

2. L'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente.

3. Per la generazione della firma digitale deve adoperarsi un certificato qualificato che, al momento della sottoscrizione, non risulti scaduto di validità ovvero non risulti revocato o sospeso.

4. Attraverso il certificato qualificato si devono rilevare, secondo le regole tecniche stabilite ai sensi dell'articolo 71, la validità del certificato stesso, nonché gli elementi identificativi del titolare e del certificatore e gli eventuali limiti d'uso.

Art. 25. Firma autenticata

1. Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma elettronica o qualsiasi altro tipo di firma avanzata autenticata dal notaio o da altro pubblico ufficiale a ciò autorizzato.

2. L'autenticazione della firma elettronica, anche mediante l'acquisizione digitale della sottoscrizione autografa, o di qualsiasi altro tipo di firma elettronica avanzata consiste nell'attestazione, da parte del pubblico ufficiale, che la firma è stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità dell'eventuale certificato elettronico utilizzato e del fatto che il documento sottoscritto non è in contrasto con l'ordinamento giuridico.

3. L'apposizione della firma digitale da parte del pubblico ufficiale ha l'efficacia di cui all'articolo 24, comma 2.

4. Se al documento informatico autenticato deve essere allegato altro documento formato in originale su altro tipo di supporto, il pubblico ufficiale può allegare copia informatica autenticata dell'originale, secondo le disposizioni dell'articolo 23, comma 5.

Art. 26. Certificatori

1. L'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva. Detti certificatori o, se persone giuridiche, i loro legali rappresentanti ed i soggetti preposti all'amministrazione, qualora emettano certificati qualificati, devono possedere i requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso le banche di cui all'articolo 26del testo unico delle leggi in materia bancaria e

creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385, e successive modificazioni.

2. L'accertamento successivo dell'assenza o del venir meno dei requisiti di cui al comma 1 comporta il divieto di prosecuzione dell'attività intrapresa.

3. Ai certificatori qualificati e ai certificatori accreditati che hanno sede stabile in altri Stati membri dell'Unione europea non si applicano le norme del presente codice e le relative norme tecniche di cui all'articolo 71 e si applicano le rispettive norme di recepimento della direttiva 1999/93/CE.

Art. 27. Certificatori qualificati

1. I certificatori che rilasciano al pubblico certificati qualificati devono trovarsi nelle condizioni previste dall'articolo 26.

2. I certificatori di cui al comma 1, devono inoltre:

a) dimostrare l'affidabilità organizzativa, tecnica e finanziaria necessaria per svolgere attività di certificazione;

b) utilizzare personale dotato delle conoscenze specifiche, dell'esperienza e delle competenze necessarie per i servizi forniti, in particolare della competenza a livello gestionale, della conoscenza specifica nel settore della tecnologia delle firme elettroniche e della dimestichezza con procedure di sicurezza appropriate e che sia in grado di rispettare le norme del presente codice e le regole tecniche di cui all'articolo 71;

c) applicare procedure e metodi amministrativi e di gestione adeguati e conformi a tecniche consolidate;

d) utilizzare sistemi affidabili e prodotti di firma protetti da alterazioni e che garantiscano la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti in ambito europeo e internazionale e certificati ai sensi dello schema nazionale di cui all'articolo 35, comma 5;

e) adottare adeguate misure contro la contraffazione dei certificati, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle chiavi private nei casi in cui il certificatore generi tali chiavi.

3. I certificatori di cui al comma 1, devono comunicare, prima dell'inizio dell'attività, anche in via telematica, una dichiarazione di inizio di attività a DigitPA, attestante l'esistenza dei presupposti e dei requisiti previsti dal presente codice.

4. DigitPA procede, d'ufficio o su segnalazione motivata di soggetti pubblici o privati, a controlli volti ad accertare la sussistenza dei presupposti e dei requisiti previsti dal presente codice e dispone, se del caso, con provvedimento motivato da notificare all'interessato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo

che, ove ciò sia possibile, l'interessato provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dall'amministrazione stessa.

Art. 28. Certificati qualificati

1. I certificati qualificati devono contenere almeno le seguenti informazioni:

a) indicazione che il certificato elettronico rilasciato è un certificato qualificato;

b) numero di serie o altro codice identificativo del certificato;

c) nome, ragione o denominazione sociale del certificatore che ha rilasciato il certificato e lo Stato nel quale è stabilito;

d) nome, cognome o uno pseudonimo chiaramente identificato come tale e codice fiscale del titolare del certificato;

e) dati per la verifica della firma, cioè i dati peculiari, come codici o chiavi crittografiche pubbliche, utilizzati per verificare la firma elettronica corrispondenti ai dati per la creazione della stessa in possesso del titolare;

f) indicazione del termine iniziale e finale del periodo di validità del certificato;

g) firma elettronica del certificatore che ha rilasciato il certificato, realizzata in conformità alle regole tecniche ed idonea a garantire l'integrità e la veridicità di tutte le informazioni contenute nel certificato medesimo.

2. In aggiunta alle informazioni di cui al comma 1, fatta salva la possibilità di utilizzare uno pseudonimo, per i titolari residenti all'estero cui non risulti attribuito il codice fiscale, si deve indicare il codice fiscale rilasciato dall'autorità fiscale del Paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di sicurezza sociale o un codice identificativo generale.

3. Il certificato qualificato può contenere, ove richiesto dal titolare o dal terzo interessato, le seguenti informazioni, se pertinenti allo scopo per il quale il certificato è richiesto:

a) le qualifiche specifiche del titolare, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;

b) i limiti d'uso del certificato, inclusi quelli derivanti dalla titolarità delle qualifiche e dai poteri di rappresentanza di cui alla lettera a) ai sensi dell'articolo 30, comma 3;

c) limiti del valore degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

3-bis. Le informazioni di cui al comma 3 possono essere contenute in un separato certificato elettronico e possono essere rese disponibili anche in rete. Con decreto del Presidente del Consiglio dei Ministri sono definite le modalità di attuazione del presente comma, anche in riferimento alle pubbliche amministrazioni e agli ordini professionali.

4. Il titolare, ovvero il terzo interessato se richiedente ai sensi del comma 3, comunicano tempestivamente al certificatore il modificarsi o venir meno delle circostanze oggetto delle informazioni di cui al presente articolo.

Art. 29. Accreditamento

1. I certificatori che intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono di essere accreditati presso DigitPA.

2. Il richiedente deve rispondere ai requisiti di cui all'articolo 27, ed allegare alla domanda oltre ai documenti indicati nel medesimo articolo il profilo professionale del personale responsabile della generazione dei dati per la creazione e per la verifica della firma, della emissione dei certificati e della gestione del registro dei certificati nonché l'impegno al rispetto delle regole tecniche.

3. Il richiedente, se soggetto privato, in aggiunta a quanto previsto dal comma 2, deve inoltre:

a) avere forma giuridica di società di capitali e un capitale sociale non inferiore a quello necessario ai fini dell'autorizzazione alla attività bancaria ai sensi dell'articolo 14 del testo unico delle leggi in materia bancaria e creditizia, di cui al decreto legislativo 1° settembre 1993, n. 385;

b) garantire il possesso, oltre che da parte dei rappresentanti legali, anche da parte dei soggetti preposti alla amministrazione e dei componenti degli organi preposti al controllo, dei requisiti di onorabilità richiesti ai soggetti che svolgono funzioni di amministrazione, direzione e controllo presso banche ai sensi dell'articolo 26 del decreto legislativo 1° settembre 1993, n. 385.

4. La domanda di accreditamento si considera accolta qualora non venga comunicato all'interessato il provvedimento di diniego entro novanta giorni dalla data di presentazione della stessa.

5. Il termine di cui al comma 4, può essere sospeso una sola volta entro trenta giorni dalla data di presentazione della domanda, esclusivamente per la motivata richiesta di documenti che integrino o completino la documentazione presentata e che non siano già nella disponibilità di DigitPA o che questo non possa acquisire autonomamente. In tale caso, il termine riprende a decorrere dalla data di ricezione della documentazione integrativa.

6. A seguito dell'accoglimento della domanda, DigitPA dispone l'iscrizione del richiedente in un apposito elenco pubblico, tenuto da DigitPA stesso e consultabile anche in via telematica, ai fini dell'applicazione della disciplina in questione.

7. Il certificatore accreditato può qualificarsi come tale nei rapporti commerciali e con le pubbliche amministrazioni.

8. Il valore giuridico delle firme elettroniche qualificate e delle firme digitali basate su certificati qualificati rilasciati da certificatori accreditati in altri Stati membri dell'Unione europea ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE è equiparato a quello previsto per le firme elettroniche qualificate e per le firme digitali basate su certificati qualificati emessi dai certificatori accreditati ai sensi del presente articolo.

9. Alle attività previste dal presente articolo si fa fronte nell'ambito delle risorse di DigitPA, senza nuovi o maggiori oneri per la finanza pubblica.

Art. 30. Responsabilità del certificatore

1. Il certificatore che rilascia al pubblico un certificato qualificato o che garantisce al pubblico l'affidabilità del certificato è responsabile, se non prova d'aver agito senza colpa o dolo, del danno cagionato a chi abbia fatto ragionevole affidamento:

a) sull'esattezza e sulla completezza delle informazioni necessarie alla verifica della firma in esso contenute alla data del rilascio e sulla loro completezza rispetto ai requisiti fissati per i certificati qualificati;

b) sulla garanzia che al momento del rilascio del certificato il firmatario detenesse i dati per la creazione della firma corrispondenti ai dati per la verifica della firma riportati o identificati nel certificato;

c) sulla garanzia che i dati per la creazione e per la verifica della firma possano essere usati in modo complementare, nei casi in cui il certificatore generi entrambi;

d) sull'adempimento degli obblighi a suo carico previsti dall'articolo 32.

2. Il certificatore che rilascia al pubblico un certificato qualificato è responsabile, nei confronti dei terzi che facciano affidamento sul certificato stesso, dei danni provocati per effetto della mancata o non tempestiva registrazione della revoca o non tempestiva sospensione del certificato, secondo quanto previsto dalle regole tecniche di cui all'articolo 71, salvo che provi d'aver agito senza colpa.

3. Il certificato qualificato può contenere limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purché i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel certificato secondo quanto previsto dalle regole tecniche di cui all'articolo 71. Il certificatore non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

Art. 31. Vigilanza sull'attività dei certificatori e dei gestori di posta elettronica certificata

1. DigitPA svolge funzioni di vigilanza e controllo sull'attività dei certificatori qualificati e dei gestori di posta elettronica certificata.

Art. 32. Obblighi del titolare e del certificatore

1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.

3. Il certificatore che rilascia, ai sensi dell'articolo 19, certificati qualificati deve inoltre:

a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;

b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;

c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;

d) attenersi alle regole tecniche di cui all'articolo 71;

e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;

[f) abrogato]

g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all'articolo 71;

h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;

i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;

j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;

k) non copiare, né conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;

l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il certificatore;

m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;

m-bis) garantire il corretto funzionamento e la continuità del sistema e comunicare immediatamente a DigitPA e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso.

4. Il certificatore è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.

5. Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

Art. 32-bis Sanzioni per i certificatori qualificati e per i gestori di posta elettronica certificata

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

2. Qualora si verifichi, fatti salvi i casi di forza maggiore o di caso fortuito, un malfunzionamento nel sistema che determini l'interruzione del servizio, ovvero la mancata o intempestiva comunicazione dello stesso disservizio a DigitPA o agli utenti, ai sensi dell'articolo 32, comma 3, lettera m-bis), DigitPA diffida il certificatore qualificato

o il gestore di posta elettronica certificata a ripristinare la regolarità del servizio o ad effettuare le comunicazioni ivi previste. Se l'interruzione del servizio ovvero la mancata o intempestiva comunicazione sono reiterati nel corso di un biennio, successivamente alla prima diffida si applica la sanzione della cancellazione dall'elenco pubblico.

3. Nei casi di cui ai commi 1 e 2 può essere applicata la sanzione amministrativa accessoria della pubblicazione dei provvedimenti di diffida o di cancellazione secondo la legislazione vigente in materia di pubblicità legale.

4. Qualora un certificatore qualificato o un gestore di posta elettronica certificata non ottemperi, nei tempi previsti, a quanto prescritto da DigitPA nell'esercizio delle attività di vigilanza di cui all'articolo 31 si applica la disposizione di cui al comma 2.

Art. 33. Uso di pseudonimi

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

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

1. Ai fini della sottoscrizione, ove prevista, di documenti informatici di rilevanza esterna, le pubbliche amministrazioni:

a) possono svolgere direttamente l'attività di rilascio dei certificati qualificati avendo a tale fine l'obbligo di accreditarsi ai sensi dell'articolo 29; tale attività può essere svolta esclusivamente nei confronti dei propri organi ed uffici, nonché di categorie di terzi, pubblici o privati. I certificati qualificati rilasciati in favore di categorie di terzi possono essere utilizzati soltanto nei rapporti con l'Amministrazione certificante, al di fuori dei quali sono privi di ogni effetto ad esclusione di quelli rilasciati da collegi e ordini professionali e relativi organi agli iscritti nei rispettivi albi e registri; con decreto del Presidente del Consiglio dei Ministri, su proposta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie e dei Ministri interessati, di concerto con il Ministro dell'economia e delle finanze, sono definite le categorie di terzi e le caratteristiche dei certificati qualificati;

b) possono rivolgersi a certificatori accreditati, secondo la vigente normativa in materia di contratti pubblici.

2. Per la formazione, gestione e sottoscrizione di documenti informatici aventi rilevanza esclusivamente interna ciascuna amministrazione può adottare, nella propria autonomia organizzativa, regole diverse da quelle contenute nelle regole tecniche di cui all'articolo 71.

3. Le regole tecniche concernenti la qualifica di pubblico ufficiale, l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni sono emanate con decreti di cui all'articolo 71 di concerto con il Ministro per la funzione pubblica, con il Ministro della giustizia e con gli altri Ministri di volta in volta interessati, sulla base dei principi generali stabiliti dai rispettivi ordinamenti.

4. Nelle more della definizione delle specifiche norme tecniche di cui al comma 3, si applicano le norme tecniche vigenti in materia di firme digitali.

5. Entro ventiquattro mesi dalla data di entrata in vigore del presente codice le pubbliche amministrazioni devono dotarsi di idonee procedure informatiche e strumenti software per la verifica delle firme digitali secondo quanto previsto dalle regole tecniche di cui all'articolo 71.

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

1. I dispositivi sicuri e le procedure utilizzate per la generazione delle firme devono presentare requisiti di sicurezza tali da garantire che la chiave privata:

a) sia riservata;

b) non possa essere derivata e che la relativa firma sia protetta da contraffazioni;

c) possa essere sufficientemente protetta dal titolare dall'uso da parte di terzi.

2. I dispositivi sicuri e le procedure di cui al comma 1 devono garantire l'integrità dei documenti informatici a cui la firma si riferisce. I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71.

3. Il secondo periodo del comma 2 non si applica alle firme apposte con procedura automatica. La firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima.

4. I dispositivi sicuri di firma devono essere dotati di certificazione di sicurezza ai sensi dello schema nazionale di cui al comma 5.

5. La conformità dei requisiti di sicurezza dei dispositivi per la creazione di una firma qualificata prescritti dall'allegato III della direttiva 1999/93/CE è accertata, in Italia, dall'Organismo di certificazione della sicurezza informatica in base allo schema nazionale per la valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione, fissato con decreto del Presidente del Consiglio dei Ministri, o, per sua delega, del Ministro per l'innovazione e le tecnologie, di concerto con i Ministri delle comunicazioni, delle attività produttive e dell'economia e delle finanze. L'attuazione dello schema nazionale non deve determinare nuovi o maggiori oneri per il bilancio dello Stato. Lo schema nazionale può prevedere altresì la valutazione e la certificazione relativamente ad ulteriori criteri europei ed internazionali, anche riguardanti altri sistemi e prodotti

afferenti al settore suddetto. La valutazione della conformità del sistema e degli strumenti di autenticazione utilizzati dal titolare delle chiavi di firma è effettuata dall'Agenzia per l'Italia digitale in conformità ad apposite linee guida da questa emanate, acquisito il parere obbligatorio dell'Organismo di certificazione della sicurezza informatica.

6. La conformità di cui al comma 5 è inoltre riconosciuta se accertata da un organismo all'uopo designato da un altro Stato membro e notificato ai sensi dell'articolo 11, paragrafo 1, lettera b), della direttiva 1999/93/CE.

Art. 36. Revoca e sospensione dei certificati qualificati

1. Il certificato qualificato deve essere a cura del certificatore:

a) revocato in caso di cessazione dell'attività del certificatore salvo quanto previsto dal comma 2 dell'articolo 37;

b) revocato o sospeso in esecuzione di un provvedimento dell'autorità;

c) revocato o sospeso a seguito di richiesta del titolare o del terzo dal quale derivano i poteri del titolare, secondo le modalità previste nel presente codice;

d) revocato o sospeso in presenza di cause limitative della capacità del titolare o di abusi o falsificazioni.

2. Il certificato qualificato può, inoltre, essere revocato o sospeso nei casi previsti dalle regole tecniche di cui all'articolo 71.

3. La revoca o la sospensione del certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene. Il momento della pubblicazione deve essere attestato mediante adeguato riferimento temporale.

4. Le modalità di revoca o sospensione sono previste nelle regole tecniche di cui all'articolo 71.

Art. 37. Cessazione dell'attività

1. Il certificatore qualificato o accreditato che intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso a DigitPA e informare senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati. (130)

2. Il certificatore di cui al comma 1 comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa. L'indicazione di un certificatore sostitutivo evita la revoca di tutti i certificati non scaduti al momento della cessazione.

3. Il certificatore di cui al comma 1 indica altro depositario del registro dei certificati e della relativa documentazione.

4. DigitPA rende nota la data di cessazione dell'attività del certificatore accreditato tramite l'elenco di cui all'articolo 29, comma 6.

4-bis. Qualora il certificatore qualificato cessi la propria attività senza indicare, ai sensi del comma 2, un certificatore sostitutivo e non si impegni a garantire la conservazione e la disponibilità della documentazione prevista dagli articoli 33 e 32, comma 3, lettera j) e delle ultime liste di revoca emesse, deve provvedere al deposito presso DigitPA che ne garantisce la conservazione e la disponibilità.

Sezione III

Trasferimenti di fondi, libri e scritture

Art. 38. Trasferimenti di fondi

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

Art. 39. Libri e scritture

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

Capo III

FORMAZIONE, GESTIONE E CONSERVAZIONE DEI DOCUMENTI INFORMATICI

Art. 40. Formazione di documenti informatici

1. Le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici secondo le disposizioni di cui al presente codice e le regole tecniche di cui all'articolo 71.

[2. abrogato]

3. Con apposito regolamento, da emanarsi entro 180 giorni dalla data di entrata in vigore del presente codice, ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, sulla proposta dei Ministri delegati per la funzione pubblica, per l'innovazione e le tecnologie e del Ministro per i beni e le attività culturali, sono individuate le categorie di documenti amministrativi che possono essere redatti in originale anche su supporto

cartaceo in relazione al particolare valore di testimonianza storica ed archivistica che sono idonei ad assumere.

4. Il Presidente del Consiglio dei Ministri, con propri decreti, fissa la data dalla quale viene riconosciuto il valore legale degli albi, elenchi, pubblici registri ed ogni altra raccolta di dati concernenti stati, qualità personali e fatti già realizzati dalle amministrazioni, su supporto informatico, in luogo dei registri cartacei.

Art. 40-bis Protocollo informatico

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

Art. 41. Procedimento e fascicolo informatico

1. Le pubbliche amministrazioni gestiscono i procedimenti amministrativi utilizzando le tecnologie dell'informazione e della comunicazione, nei casi e nei modi previsti dalla normativa vigente.

1-bis. La gestione dei procedimenti amministrativi è attuata in modo da consentire, mediante strumenti automatici, il rispetto di quanto previsto all'articolo 54, commi 2-ter e 2-quater.

2. La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241.

2-bis. Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento. Le regole per la costituzione, l'identificazione e l'utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico ed il sistema pubblico di connettività, e comunque rispettano i criteri dell'interoperabilità e della cooperazione applicativa; regole tecniche specifiche possono essere dettate ai sensi dell'articolo 71, di concerto con il Ministro della funzione pubblica.

2-ter. Il fascicolo informatico reca l'indicazione:

a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;

b) delle altre amministrazioni partecipanti;

c) del responsabile del procedimento;

d) dell'oggetto del procedimento;

e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater;

e-bis) dell'identificativo del fascicolo medesimo.

2-quater. Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990.

3. Ai sensi degli articoli da 14 a 14-quinquies della legge 7 agosto 1990, n. 241, previo accordo tra le amministrazioni coinvolte, la conferenza dei servizi è convocata e svolta avvalendosi degli strumenti informatici disponibili, secondo i tempi e le modalità stabiliti dalle amministrazioni medesime.

Art. 42. Dematerializzazione dei documenti delle pubbliche amministrazioni

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

Art. 43. Riproduzione e conservazione dei documenti

1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali.

3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n. 42.

Art. 44. Requisiti per la conservazione dei documenti informatici

1. Il sistema di conservazione dei documenti informatici assicura:

a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

b) l'integrità del documento;

c) la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;

d) il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in allegato B a tale decreto.

1-bis. Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, e, ove previsto, con il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza. (147)

1-ter. Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito dall'articolo 43 e dalle regole tecniche ivi previste, nonché dal comma 1 ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche.

Art. 44-bis Conservatori accreditati

1. I soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi anche per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza, chiedono l'accreditamento presso DigitPA.

2. Si applicano, in quanto compatibili, gli articoli 26, 27, 29, ad eccezione del comma 3, lettera a) e 31.

3. I soggetti privati di cui al comma 1 sono costituiti in società di capitali con capitale sociale non inferiore a euro 200.000.

Capo IV

TRASMISSIONE INFORMATICA DEI DOCUMENTI

Art. 45. Valore giuridico della trasmissione

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

2. Il documento informatico trasmesso per via telematica si intende spedito dal mittente se inviato al proprio gestore, e si intende consegnato al destinatario se reso disponibile all'indirizzo elettronico da questi dichiarato, nella casella di posta elettronica del destinatario messa a disposizione dal gestore.

Art. 46. Dati particolari contenuti nei documenti trasmessi

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

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

1. Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono mediante l'utilizzo della posta elettronica o in cooperazione applicativa; esse sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza.

1-bis. L'inosservanza della disposizione di cui al comma 1, ferma restando l'eventuale responsabilità per danno erariale, comporta responsabilità dirigenziale e responsabilità disciplinare.

2. Ai fini della verifica della provenienza le comunicazioni sono valide se:

a) sono sottoscritte con firma digitale o altro tipo di firma elettronica qualificata;

b) ovvero sono dotate di segnatura di protocollo di cui all'articolo 55 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;

c) ovvero è comunque possibile accertarne altrimenti la provenienza, secondo quanto previsto dalla normativa vigente o dalle regole tecniche di cui all'articolo 71. È in ogni caso esclusa la trasmissione di documenti a mezzo fax;

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

3. Le pubbliche amministrazioni e gli altri soggetti di cui all'articolo 2, comma 2, provvedono ad istituire e pubblicare nell'Indice PA almeno una casella di posta elettronica certificata per ciascun registro di protocollo. La pubbliche amministrazioni utilizzano per le comunicazioni tra l'amministrazione ed i propri dipendenti la posta elettronica o altri strumenti informatici di comunicazione nel rispetto delle norme in materia di protezione dei dati personali e previa informativa agli interessati in merito al grado di riservatezza degli strumenti utilizzati.

Art. 48. Posta elettronica certificata

1. La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata ai sensi del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, o mediante altre soluzioni tecnologiche individuate con decreto del Presidente del Consiglio dei Ministri, sentito DigitPA.

2. La trasmissione del documento informatico per via telematica, effettuata ai sensi del comma 1, equivale, salvo che la legge disponga diversamente, alla notificazione per mezzo della posta.

3. La data e l'ora di trasmissione e di ricezione di un documento informatico trasmesso ai sensi del comma 1 sono opponibili ai terzi se conformi alle disposizioni di cui al decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, ed alle relative regole tecniche, ovvero conformi al decreto del Presidente del Consiglio dei Ministri di cui al comma 1.

Art. 49. Segretezza della corrispondenza trasmessa per via telematica

1. Gli addetti alle operazioni di trasmissione per via telematica di atti, dati e documenti formati con strumenti informatici non possono prendere cognizione della corrispondenza telematica, duplicare con qualsiasi mezzo o cedere a terzi a qualsiasi titolo informazioni anche in forma sintetica o per estratto sull'esistenza o sul contenuto di corrispondenza, comunicazioni o messaggi trasmessi per via telematica, salvo che si tratti di informazioni per loro natura o per espressa indicazione del mittente destinate ad essere rese pubbliche.

2. Agli effetti del presente codice, gli atti, i dati e i documenti trasmessi per via telematica si considerano, nei confronti del gestore del sistema di trasporto delle informazioni, di proprietà del mittente sino a che non sia avvenuta la consegna al destinatario.

Capo V

DATI DELLE PUBBLICHE AMMINISTRAZIONI E SERVIZI IN RETE

Sezione I

Dati delle pubbliche amministrazioni

Art. 50. Disponibilità dei dati delle pubbliche amministrazioni

1. I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico.

2. Qualunque dato trattato da una pubblica amministrazione, con le esclusioni di cui all'articolo 2, comma 6, salvi i casi previsti dall'articolo 24 della legge 7 agosto 1990, n. 241, e nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di quest'ultima, salvo per la prestazione di elaborazioni aggiuntive; è fatto comunque salvo il disposto dell'articolo 43, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

3. Al fine di rendere possibile l'utilizzo in via telematica dei dati di una pubblica amministrazione da parte dei sistemi informatici di altre amministrazioni l'amministrazione titolare dei dati predispone, gestisce ed eroga i servizi informatici allo scopo necessari, secondo le regole tecniche del sistema pubblico di connettività di cui al presente decreto.

Art. 50-bis Continuità operativa

1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono:

a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali,

tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.

Art. 51. Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni

1. Con le regole tecniche adottate ai sensi dell'articolo 71 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.

1-bis. DigitPA, ai fini dell'attuazione del comma 1:

a) raccorda le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici;

b) promuove intese con le analoghe strutture internazionali;

c) segnala al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche di cui al comma 1 da parte delle pubbliche amministrazioni.

2. I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta.

2-bis. Le amministrazioni hanno l'obbligo di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi.

Art. 52. Accesso telematico e riutilizzo dei dati delle pubbliche amministrazioni

1. L'accesso telematico a dati, documenti e procedimenti e il riutilizzo dei dati e documenti è disciplinato dai soggetti di cui all'articolo 2, comma 2, secondo le disposizioni del presente codice e nel rispetto della normativa vigente. Le pubbliche amministrazioni pubblicano nel proprio sito web, all'interno della sezione «Trasparenza, valutazione e merito», il catalogo dei dati, dei metadati e delle relative banche dati in loro

possesso ed i regolamenti che ne disciplinano l'esercizio della facoltà di accesso telematico e il riutilizzo, fatti salvi i dati presenti in Anagrafe tributaria.

2. I dati e i documenti che le amministrazioni titolari pubblicano, con qualsiasi modalità, senza l'espressa adozione di una licenza di cui all'articolo 2, comma 1, lettera h), del decreto legislativo 24 gennaio 2006, n. 36, si intendono rilasciati come dati di tipo aperto ai sensi all'articolo 68, comma 3, del presente Codice. L'eventuale adozione di una licenza di cui al citato articolo 2, comma 1, lettera h), è motivata ai sensi delle linee guida nazionali di cui al comma 7.

3. Nella definizione dei capitolati o degli schemi dei contratti di appalto relativi a prodotti e servizi che comportino la raccolta e la gestione di dati pubblici, le pubbliche amministrazioni di cui all'articolo 2, comma 2, prevedono clausole idonee a consentire l'accesso telematico e il riutilizzo, da parte di persone fisiche e giuridiche, di tali dati, dei metadati, degli schemi delle strutture di dati e delle relative banche dati.

4. Le attività volte a garantire l'accesso telematico e il riutilizzo dei dati delle pubbliche amministrazioni rientrano tra i parametri di valutazione della performance dirigenziale ai sensi dell'articolo 11, comma 9, del decreto legislativo 27 ottobre 2009, n. 150.

5. L'Agenzia per l'Italia digitale promuove le politiche di valorizzazione del patrimonio informativo pubblico nazionale e attua le disposizioni di cui al capo V del presente Codice.

6. Entro il mese di febbraio di ogni anno l'Agenzia trasmette al Presidente del Consiglio dei Ministri o al Ministro delegato per l'innovazione tecnologica, che li approva entro il mese successivo, un'Agenda nazionale in cui definisce contenuti e gli obiettivi delle politiche di valorizzazione del patrimonio informativo pubblico e un rapporto annuale sullo stato del processo di valorizzazione in Italia; tale rapporto è pubblicato in formato aperto sul sito istituzionale della Presidenza del Consiglio dei Ministri.

7. L'Agenzia definisce e aggiorna annualmente le linee guida nazionali che individuano gli standard tecnici, compresa la determinazione delle ontologie dei servizi e dei dati, le procedure e le modalità di attuazione delle disposizioni del Capo V del presente Codice con l'obiettivo di rendere il processo omogeneo a livello nazionale, efficiente ed efficace. Le pubbliche amministrazioni di cui all'articolo 2, comma 2, del presente Codice si uniformano alle suddette linee guida.

8. Il Presidente del Consiglio o il Ministro delegato per l'innovazione tecnologica riferisce annualmente al Parlamento sullo stato di attuazione delle disposizioni del presente articolo.

9. L'Agenzia svolge le attività indicate dal presente articolo con le risorse umane, strumentali, e finanziarie previste a legislazione vigente.

Art. 53. Caratteristiche dei siti

1. Le pubbliche amministrazioni centrali realizzano siti istituzionali su reti telematiche che rispettano i principi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili, completezza di informazione, chiarezza di linguaggio, affidabilità, semplicità dì consultazione, qualità, omogeneità ed interoperabilità. Sono in particolare resi facilmente reperibili e consultabili i dati di cui all'articolo 54.

2. DigitPA svolge funzioni consultive e di coordinamento sulla realizzazione e modificazione dei siti delle amministrazioni centrali.

3. Lo Stato promuove intese ed azioni comuni con le regioni e le autonomie locali affinché realizzino siti istituzionali con le caratteristiche di cui al comma 1.

Art. 54. Contenuto dei siti delle pubbliche amministrazioni

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

Art. 55. Consultazione delle iniziative normative del Governo

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

2. Con decreto del Presidente del Consiglio dei Ministri sono individuate le modalità di partecipazione del cittadino alla consultazione gratuita in via telematica.

Art. 56. Dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado

1. I dati identificativi delle questioni pendenti dinanzi al giudice amministrativo e contabile sono resi accessibili a chi vi abbia interesse mediante pubblicazione sul sistema informativo interno e sul sito istituzionale delle autorità emananti.

2. Le sentenze e le altre decisioni del giudice amministrativo e contabile, rese pubbliche mediante deposito in segreteria, sono contestualmente inserite nel sistema informativo interno e sul sito istituzionale, osservando le cautele previste dalla normativa in materia di tutela dei dati personali.

2-bis. I dati identificativi delle questioni pendenti, le sentenze e le altre decisioni depositate in cancelleria o segreteria dell'autorità giudiziaria di ogni ordine e grado sono, comunque, rese accessibili ai sensi dell'articolo 51 del codice in materia di protezione dei dati personali approvato con decreto legislativo n. 196 del 2003.

Art. 57. Moduli e formulari [abrogato]

Art. 57-bis. Indice degli indirizzi delle pubbliche amministrazioni

1. Al fine di assicurare la pubblicità dei riferimenti telematici delle pubbliche amministrazioni e dei gestori dei pubblici servizi è istituito l'indice degli indirizzi della pubblica amministrazione e dei gestori di pubblici servizi, nel quale sono indicati gli indirizzi di posta elettronica certificata da utilizzare per le comunicazioni e per lo scambio di informazioni e per l'invio di documenti a tutti gli effetti di legge tra le pubbliche amministrazioni, i gestori di pubblici servizi ed i privati.

2. La realizzazione e la gestione dell'indice sono affidate a DigitPA, che può utilizzare a tal fine elenchi e repertori già formati dalle amministrazioni pubbliche.

3. Le amministrazioni aggiornano gli indirizzi e i contenuti dell'indice tempestivamente e comunque con cadenza almeno semestrale secondo le indicazioni di DigitPA. La mancata comunicazione degli elementi necessari al completamento dell'indice e del loro aggiornamento è valutata ai fini della responsabilità dirigenziale e dell'attribuzione della retribuzione di risultato ai dirigenti responsabili.

Sezione II

Fruibilità dei dati

Art. 58. Modalità della fruibilità del dato

1. Il trasferimento di un dato da un sistema informativo ad un altro non modifica la titolarità del dato.

2. Ai sensi dell'articolo 50, comma 2, nonché al fine di agevolare l'acquisizione d'ufficio ed il controllo sulle dichiarazioni sostitutive riguardanti informazioni e dati relativi a stati, qualità personali e fatti di cui agli articoli 46 e 47 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le Amministrazioni titolari di banche dati accessibili per via telematica predispongono, sulla base delle linee guida redatte da DigitPA, sentito il Garante per la protezione dei dati personali, apposite convenzioni aperte all'adesione di tutte le amministrazioni interessate volte a disciplinare le modalità di accesso ai dati da parte delle stesse amministrazioni procedenti, senza oneri a loro carico. Le convenzioni valgono anche quale autorizzazione ai sensi dell'articolo 43, comma 2, del citato decreto del Presidente della Repubblica n. 445 del 2000.

3. DigitPA provvede al monitoraggio dell'attuazione del presente articolo, riferendo annualmente con apposita relazione al Ministro per la pubblica amministrazione e l'innovazione e alla Commissione per la valutazione, la trasparenza e l'integrità delle amministrazione pubbliche di cui all'articolo 13 del decreto legislativo 27 ottobre 2009, n. 150.

3-bis. In caso di mancata predisposizione delle convenzioni di cui al comma 2, il Presidente del Consiglio dei Ministri stabilisce un termine entro il quale le amministrazioni interessate devono provvedere. Decorso inutilmente il termine, il Presidente del Consiglio dei Ministri può nominare un commissario ad acta incaricato di predisporre le predette convenzioni. Al Commissario non spettano compensi, indennità o rimborsi. (189)

3-ter. Resta ferma la speciale disciplina dettata in materia di dati territoriali.

Art. 59. Dati territoriali

1. Per dato territoriale si intende qualunque informazione geograficamente localizzata.

2. E' istituito il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, con il compito di definire le regole tecniche per la realizzazione delle basi dei dati territoriali, la documentazione, la fruibilità e lo scambio dei dati stessi tra le pubbliche amministrazioni centrali e locali in coerenza con le disposizioni del presente decreto che disciplinano il sistema pubblico di connettività.

3. Per agevolare la pubblicità dei dati di interesse generale, disponibili presso le pubbliche amministrazioni a livello nazionale, regionale e locale, presso DigitPA è istituito il Repertorio nazionale dei dati territoriali.

4. Ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, con uno o più decreti sulla proposta del Presidente del Consiglio dei Ministri o, per sua delega, del Ministro per l'innovazione e le tecnologie, previa intesa con la Conferenza unificata di cui all'articolo 8 decreto legislativo 28 agosto 1997, n. 281, sono definite la composizione e le modalità per il funzionamento del Comitato di cui al comma 2.

5. Con decreti del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con il Ministro dell'ambiente e della tutela del territorio e del mare, per i profili relativi ai dati ambientali, sentito il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni, e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 luglio 1998, n. 281, sono definite le regole tecniche per la definizione del contenuto del repertorio nazionale dei dati territoriali, nonché delle modalità di prima costituzione e di successivo aggiornamento dello stesso, per la formazione, la documentazione e lo scambio dei dati territoriali detenuti dalle singole amministrazioni competenti, nonché le regole ed i costi per l'utilizzo dei dati stessi tra le pubbliche amministrazioni centrali e locali e da parte dei privati.

6. La partecipazione al Comitato non comporta oneri né alcun tipo di spese ivi compresi compensi o gettoni di presenza. Gli eventuali rimborsi per spese di viaggio sono a carico delle amministrazioni direttamente interessate che vi provvedono nell'ambito degli ordinari stanziamenti di bilancio.

7. Agli oneri finanziari di cui al comma 3 si provvede con il fondo di finanziamento per i progetti strategici del settore informatico di cui all'articolo 27, comma 2, della legge 16 gennaio 2003, n. 3.

7-bis. Nell'ambito dei dati territoriali di interesse nazionale rientra la base dei dati catastali gestita dall'Agenzia del territorio. Per garantire la circolazione e la fruizione dei dati catastali conformemente alle finalità ed alle condizioni stabilite dall'articolo 50, il direttore dell'Agenzia del territorio, di concerto con il Comitato per le regole tecniche sui dati territoriali delle pubbliche amministrazioni e previa intesa con la Conferenza unificata, definisce con proprio decreto entro la data del 30 giugno 2006, in coerenza con le disposizioni che disciplinano il sistema pubblico di connettività, le regole tecnico-economiche per l'utilizzo dei dati catastali per via telematica da parte dei sistemi informatici di altre amministrazioni.

Art. 60. Base di dati di interesse nazionale

1. Si definisce base di dati di interesse nazionale l'insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è utilizzabile dalle pubbliche amministrazioni, anche per fini statistici, per l'esercizio delle proprie funzioni e nel rispetto delle competenze e delle normative vigenti.

2. Ferme le competenze di ciascuna pubblica amministrazione, le basi di dati di interesse nazionale costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate. La realizzazione di tali sistemi informativi e le modalità di aggiornamento sono attuate secondo le regole tecniche sul sistema pubblico di connettività di cui all'articolo 73 e secondo le vigenti regole del Sistema statistico nazionale di cui al decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni.

3. Le basi di dati di interesse nazionale sono individuate con decreto del Presidente del Consiglio dei Ministri, su proposta del Presidente del Consiglio dei Ministri o del Ministro delegato per l'innovazione e le tecnologie, di concerto con i Ministri di volta in volta interessati, d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, nelle materie di competenza e sentiti il Garante per la protezione dei dati personali e l'Istituto nazionale di statistica. Con il medesimo decreto sono altresì individuate le strutture responsabili della gestione operativa di ciascuna base di dati e le caratteristiche tecniche del sistema informativo di cui al comma 2.

3-bis. In sede di prima applicazione e fino all'adozione del decreto di cui al comma 3, sono individuate le seguenti basi di dati di interesse nazionale:

a) repertorio nazionale dei dati territoriali;

b) anagrafe nazionale della popolazione residente;

c) banca dati nazionale dei contratti pubblici di cui all'articolo 62-bis;

d) casellario giudiziale;

e) registro delle imprese;

f) gli archivi automatizzati in materia di immigrazione e di asilo di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 27 luglio 2004, n. 242,

f-bis) Anagrafe nazionale degli assistiti (ANA).

4. Agli oneri finanziari di cui al presente articolo si provvede con il fondo di finanziamento per i progetti strategici del settore informatico di cui all'articolo 27, comma 2, della legge 16 gennaio 2003, n. 3.

Art. 61. Delocalizzazione dei registri informatici

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

Art. 62. Anagrafe nazionale della popolazione residente - ANPR

1. È istituita presso il Ministero dell'interno l'Anagrafe nazionale della popolazione residente (ANPR), quale base di dati di interesse nazionale, ai sensi dell'articolo 60, che subentra all'Indice nazionale delle anagrafi (INA), istituito ai sensi del quinto comma dell'articolo 1 della legge 24 dicembre 1954, n. 1228, recante «Ordinamento delle anagrafi della popolazione residente» e all'Anagrafe della popolazione italiana residente all'estero (AIRE), istituita ai sensi della legge 27 ottobre 1988, n. 470, recante «Anagrafe e censimento degli italiani all'estero». Tale base di dati è sottoposta ad un audit di sicurezza con cadenza annuale in conformità alle regole tecniche di cui all'articolo 51. I risultati dell'audit sono inseriti nella relazione annuale del Garante per la protezione dei dati personali.

2. Ferme restando le attribuzioni del sindaco di cui all'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali, approvato con il decreto legislativo 18 agosto 2000, n. 267, l'ANPR subentra altresì alle anagrafi della popolazione residente

e dei cittadini italiani residenti all'estero tenute dai comuni. Con il decreto di cui al comma 6 è definito un piano per il graduale subentro dell'ANPR alle citate anagrafi, da completare entro il 31 dicembre 2014. Fino alla completa attuazione di detto piano, l'ANPR acquisisce automaticamente in via telematica i dati contenuti nelle anagrafi tenute dai comuni per i quali non è ancora avvenuto il subentro. L'ANPR è organizzata secondo modalità funzionali e operative che garantiscono la univocità dei dati stessi.

3. L'ANPR assicura al singolo comune la disponibilità dei dati anagrafici della popolazione residente e degli strumenti per lo svolgimento delle funzioni di competenza statale attribuite al sindaco ai sensi dell'articolo 54, comma 3, del testo unico delle leggi sull'ordinamento degli enti locali di cui al decreto legislativo 18 agosto 2000, n. 267, nonché la disponibilità dei dati anagrafici e dei servizi per l'interoperabilità con le banche dati tenute dai comuni per lo svolgimento delle funzioni di competenza. L'ANPR consente esclusivamente ai comuni la certificazione dei dati anagrafici nel rispetto di quanto previsto dall'articolo 33 del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, anche in modalità telematica. I comuni inoltre possono consentire, anche mediante apposite convenzioni, la fruizione dei dati anagrafici da parte dei soggetti aventi diritto. L'ANPR assicura alle pubbliche amministrazioni e agli organismi che erogano pubblici servizi l'accesso ai dati contenuti nell'ANPR.

4. Con il decreto di cui al comma 6 sono disciplinate le modalità di integrazione nell'ANPR dei dati dei cittadini attualmente registrati in anagrafi istituite presso altre amministrazioni nonché dei dati relativi al numero e alla data di emissione e di scadenza della carta di identità della popolazione residente.

5. Ai fini della gestione e della raccolta informatizzata di dati dei cittadini, le pubbliche amministrazioni di cui all'articolo 2, comma 2, del presente Codice si avvalgono esclusivamente dell'ANPR, che viene integrata con gli ulteriori dati a tal fine necessari.

6. Con uno o più decreti del Presidente del Consiglio dei Ministri, su proposta del Ministro dell'interno, del Ministro per la pubblica amministrazione e la semplificazione e del Ministro delegato all'innovazione tecnologica, di concerto con il Ministro dell'economia e delle finanze, d'intesa con l'Agenzia per l'Italia digitale, la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano nonché con la Conferenza Stato - città, di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, per gli aspetti d'interesse dei comuni, sentita l'ISTAT e acquisito il parere del Garante per la protezione dei dati personali, sono stabiliti i tempi e le modalità di attuazione delle disposizioni del presente articolo, anche con riferimento:

a) alle garanzie e alle misure di sicurezza da adottare nel trattamento dei dati personali, alle modalità e ai tempi di conservazione dei dati e all'accesso ai dati da parte delle pubbliche amministrazioni per le proprie finalità istituzionali secondo le modalità di cui all'articolo 58;

b) ai criteri per l'interoperabilità dell'ANPR con le altre banche dati di rilevanza nazionale e regionale, secondo le regole tecniche del sistema pubblico di connettività di cui al capo VIII del presente decreto, in modo che le informazioni di anagrafe, una volta rese dai

cittadini, si intendano acquisite dalle pubbliche amministrazioni senza necessità di ulteriori adempimenti o duplicazioni da parte degli stessi;

c) all'erogazione di altri servizi resi disponibili dall'ANPR, tra i quali il servizio di invio telematico delle attestazioni e delle dichiarazioni di nascita e dei certificati di cui all'articolo 74 del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, compatibile con il sistema di trasmissione di cui al decreto del Ministro della salute in data 26 febbraio 2010, pubblicato nella Gazzetta Ufficiale n. 65 del 19 marzo 2010.

Art. 62-bis Banca dati nazionale dei contratti pubblici

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

Art. 62-ter Anagrafe nazionale degli assistiti

1. Per rafforzare gli interventi in tema di monitoraggio della spesa del settore sanitario, accelerare il processo di automazione amministrativa e migliorare i servizi per i cittadini e le pubbliche amministrazioni, è istituita, nell'ambito del sistema informativo realizzato dal Ministero dell'economia e delle finanze in attuazione di quanto disposto dall'articolo 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, l'Anagrafe nazionale degli assistiti (ANA).

2. L'ANA, realizzata dal Ministero dell'economia e delle finanze, in accordo con il Ministero della salute in relazione alle specifiche esigenze di monitoraggio dei livelli essenziali di assistenza (LEA), nel rispetto delle previsioni di cui al comma 5 dell'articolo 62 del presente decreto, subentra, per tutte le finalità previste dalla normativa vigente, alle anagrafi e agli elenchi degli assistiti tenuti dalle singole aziende sanitarie locali, ai sensi dell'articolo 7 della legge 7 agosto 1982, n. 526, che mantengono la titolarità dei dati di propria competenza e ne assicurano l'aggiornamento.

3. L'ANA assicura alla singola azienda sanitaria locale la disponibilità dei dati e degli strumenti per lo svolgimento delle funzioni di propria competenza e garantisce l'accesso ai dati in essa contenuti da parte delle pubbliche amministrazioni per le relative finalità istituzionali, secondo le modalità di cui all'articolo 58, comma 2, del presente decreto.

4. Con il subentro dell'ANA, l'azienda sanitaria locale cessa di fornire ai cittadini il libretto sanitario personale previsto dall'articolo 27 della legge 23 dicembre 1978, n. 833.

È facoltà dei cittadini di accedere in rete ai propri dati contenuti nell'ANA, secondo le modalità di cui al comma 1 dell'articolo 6 del presente decreto, ovvero di richiedere presso l'azienda sanitaria locale competente copia cartacea degli stessi.

5. In caso di trasferimento di residenza del cittadino, l'ANA ne dà immediata comunicazione in modalità telematica alle aziende sanitarie locali interessate dal trasferimento. L'azienda sanitaria locale nel cui territorio è compresa la nuova residenza provvede alla presa in carico del cittadino, nonché all'aggiornamento dell'ANA per i dati di propria competenza. Nessun'altra comunicazione in merito al trasferimento di residenza è dovuta dal cittadino alle aziende sanitarie locali interessate.

6. L'ANA assicura al nuovo sistema informativo sanitario nazionale realizzato dal Ministero della salute in attuazione di quanto disposto dall'articolo 87 della legge 23 dicembre 2000, n. 388, con le modalità definite dal decreto del Presidente del Consiglio dei ministri di cui al comma 7, l'accesso ai dati e la disponibilità degli strumenti funzionali a garantire l'appropriatezza e l'efficacia delle prestazioni di cura erogate al cittadino, nonché per le finalità di cui all'articolo 15, comma 25-bis, del decreto-legge 6 luglio 2012, n. 95, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 135.

7. Entro il 30 giugno 2014, con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro della salute e del Ministro dell'economia e delle finanze, previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, sono stabiliti:

a) i contenuti dell'ANA, tra i quali devono essere inclusi il medico di medicina generale, il codice esenzione e il domicilio;

b) il piano per il graduale subentro dell'ANA alle anagrafi e agli elenchi degli assistiti tenuti dalle singole aziende sanitarie locali, da completare entro il 30 giugno 2015;

c) le garanzie e le misure di sicurezza da adottare, i criteri per l'interoperabilità dell'ANA con le altre banche dati di rilevanza nazionale e regionale, nonché le modalità di cooperazione dell'ANA con banche dati già istituite a livello regionale per le medesime finalità, nel rispetto della normativa sulla protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, e delle regole tecniche del sistema pubblico di connettività, ai sensi del presente decreto.

Sezione III

Servizi in rete

Art. 63. Organizzazione e finalità dei servizi in rete

1. Le pubbliche amministrazioni centrali individuano le modalità di erogazione dei servizi in rete in base a criteri di valutazione di efficacia, economicità ed utilità e nel rispetto dei principi di eguaglianza e non discriminazione, tenendo comunque presenti le

dimensioni dell'utenza, la frequenza dell'uso e l'eventuale destinazione all'utilizzazione da parte di categorie in situazioni di disagio.

2. Le pubbliche amministrazioni e i gestori di servizi pubblici progettano e realizzano i servizi in rete mirando alla migliore soddisfazione delle esigenze degli utenti, in particolare garantendo la completezza del procedimento, la certificazione dell'esito e l'accertamento del grado di soddisfazione dell'utente. A tal fine, sono tenuti ad adottare strumenti idonei alla rilevazione immediata, continua e sicura del giudizio degli utenti, in conformità alle regole tecniche da emanare ai sensi dell'articolo 71. Per le amministrazioni e i gestori di servizi pubblici regionali e locali le regole tecniche sono adottate previo parere della Commissione permanente per l'innovazione tecnologica nelle regioni e negli enti locali di cui all'articolo 14, comma 3-bis.

3. Le pubbliche amministrazioni collaborano per integrare i procedimenti di rispettiva competenza al fine di agevolare gli adempimenti di cittadini ed imprese e rendere più efficienti i procedimenti che interessano più amministrazioni, attraverso idonei sistemi di cooperazione.

3-bis. A partire dal 1° gennaio 2014, allo scopo di incentivare e favorire il processo di informatizzazione e di potenziare ed estendere i servizi telematici, i soggetti di cui all'articolo 2, comma 2, utilizzano esclusivamente i canali e i servizi telematici, ivi inclusa la posta elettronica certificata, per l'utilizzo dei propri servizi, anche a mezzo di intermediari abilitati, per la presentazione da parte degli interessati di denunce, istanze e atti e garanzie fideiussorie, per l'esecuzione di versamenti fiscali, contributivi, previdenziali, assistenziali e assicurativi, nonché per la richiesta di attestazioni e certificazioni.

3-ter. A partire dal 1° gennaio 2014 i soggetti indicati al comma 3-bis utilizzano esclusivamente servizi telematici o la posta elettronica certificata anche per gli atti, le comunicazioni o i servizi dagli stessi resi.

3-quater. I soggetti indicati al comma 3-bis, almeno sessanta giorni prima della data della loro entrata in vigore, pubblicano nel sito web istituzionale l'elenco dei provvedimenti adottati ai sensi dei commi 3-bis e 3-ter, nonché termini e modalità di utilizzo dei servizi e dei canali telematici e della posta elettronica certificata.

3-quinquies. Con decreto del Presidente del Consiglio dei Ministri, sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e successive modificazioni, da emanare entro sei mesi dalla data di entrata in vigore della presente disposizione, sono stabilite le deroghe e le eventuali limitazioni al principio di esclusività indicato dal comma 3-bis, anche al fine di escludere l'insorgenza di nuovi o maggiori oneri per la finanza pubblica.

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

1. La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica.

2. Le pubbliche amministrazioni possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio. Con l'istituzione del sistema SPID di cui al comma 2-bis, le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi solo mediante gli strumenti di cui al comma 1, ovvero mediante servizi offerti dal medesimo sistema SPID. L'accesso con carta d'identità elettronica e carta nazionale dei servizi è comunque consentito indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

2-bis. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).

2-ter Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale, secondo modalità definite con il decreto di cui al comma 2-sexies, gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati.

2-quater. Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-sexies.

2-quinquies. Ai fini dell'erogazione dei propri servizi in rete, è altresì riconosciuta alle imprese, secondo le modalità definite con il decreto di cui al comma 2-sexies, la facoltà di avvalersi del sistema SPID per la gestione dell'identità digitale dei propri utenti. L'adesione al sistema SPID per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera l'impresa da un obbligo generale di sorveglianza delle attività sui propri siti, ai sensi dell'articolo 17 del decreto legislativo 9 aprile 2003, n. 70.

2-sexies. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro delegato per l'innovazione tecnologica e del Ministro per la pubblica amministrazione e la semplificazione, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali, sono definite le caratteristiche del sistema SPID, anche con riferimento:

a) al modello architetturale e organizzativo del sistema;

b) alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;

c) agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese, compresi gli strumenti di cui al comma 1;

d) alle modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;

e) ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;

f) alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete.

[3. abrogato]

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

1. Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici ai sensi dell'articolo 38, commi 1 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, sono valide:

a) se sottoscritte mediante la firma digitale o la firma elettronica qualificata, il cui certificato è rilasciato da un certificatore accreditato;

b) ovvero, quando l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi, nei limiti di quanto stabilito da ciascuna amministrazione ai sensi della normativa vigente;

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

c-bis) ovvero se trasmesse dall'autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite con regole tecniche adottate ai sensi dell'articolo 71, e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato. In tal caso, la trasmissione costituisce dichiarazione vincolante ai sensi dell'articolo 6, comma 1, secondo periodo. Sono fatte salve le disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario.

1-bis. Con decreto del Ministro per la pubblica amministrazione e l'innovazione e del Ministro per la semplificazione normativa, su proposta dei Ministri competenti per

materia, possono essere individuati i casi in cui è richiesta la sottoscrizione mediante firma digitale.

1-ter. Il mancato avvio del procedimento da parte del titolare dell'ufficio competente a seguito di istanza o dichiarazione inviate ai sensi e con le modalità di cui al comma 1, lettere a), c) e c-bis), comporta responsabilità dirigenziale e responsabilità disciplinare dello stesso.

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

[3. abrogato]

4. Il comma 2 dell'articolo 38 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è sostituito dal seguente:

«2. Le istanze e le dichiarazioni inviate per via telematica sono valide se effettuate secondo quanto previsto dall'articolo 65 del decreto legislativo 7 marzo 2005, n. 82».

Sezione IV

Carte elettroniche

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

1. Le caratteristiche e le modalità per il rilascio della carta d'identità elettronica, e dell'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento dell'età prevista dalla legge per il rilascio della carta d'identità elettronica, sono definite con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Ministro dell'interno, di concerto con il Ministro per la funzione pubblica, con il Ministro per l'innovazione e le tecnologie e con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281. (225)

2. Le caratteristiche e le modalità per il rilascio, per la diffusione e l'uso della carta nazionale dei servizi sono definite con uno o più regolamenti, ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, adottati su proposta congiunta dei Ministri per la funzione pubblica e per l'innovazione e le tecnologie, di concerto con il Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, nel rispetto dei seguenti principi:

a) all'emissione della carta nazionale dei servizi provvedono, su richiesta del soggetto interessato, le pubbliche amministrazioni che intendono rilasciarla;

b) l'onere economico di produzione e rilascio della carta nazionale dei servizi è a carico delle singole amministrazioni che la emettono;

c) eventuali indicazioni di carattere individuale connesse all'erogazione dei servizi al cittadino, sono possibili nei limiti di cui al decreto legislativo 30 giugno 2003, n. 196;

d) le pubbliche amministrazioni che erogano servizi in rete devono consentirne l'accesso ai titolari della carta nazionale dei servizi indipendentemente dall'ente di emissione, che è responsabile del suo rilascio;

e) la carta nazionale dei servizi può essere utilizzata anche per i pagamenti informatici tra soggetti privati e pubbliche amministrazioni, secondo quanto previsto dalla normativa vigente.

3. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento dell'età prevista dalla legge per il rilascio della carta d'identità elettronica, devono contenere:

a) i dati identificativi della persona;

b) il codice fiscale.

4. La carta d'identità elettronica e l'analogo documento, rilasciato a seguito della denuncia di nascita e prima del compimento dell'età prevista dalla legge per il rilascio della carta d'identità elettronica, possono contenere, a richiesta dell'interessato ove si tratti di dati sensibili:

a) l'indicazione del gruppo sanguigno;

b) le opzioni di carattere sanitario previste dalla legge;

c) i dati biometrici indicati col decreto di cui al comma 1, con esclusione, in ogni caso, del DNA;

d) tutti gli altri dati utili al fine di razionalizzare e semplificare l'azione amministrativa e i servizi resi al cittadino, anche per mezzo dei portali, nel rispetto della normativa in materia di riservatezza;

e) le procedure informatiche e le informazioni che possono o debbono essere conosciute dalla pubblica amministrazione e da altri soggetti, occorrenti per la firma elettronica.

5. La carta d'identità elettronica e la carta nazionale dei servizi possono essere utilizzate quali strumenti di autenticazione telematica per l'effettuazione di pagamenti tra soggetti privati e pubbliche amministrazioni, secondo le modalità stabilite con le regole tecniche di cui all'articolo 71, di concerto con il Ministro dell'economia e delle finanze, sentita la Banca d'Italia.

6. Con decreto del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e delle finanze, sentito il Garante per la protezione dei dati personali e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, sono dettate le regole tecniche e di sicurezza relative alle

tecnologie e ai materiali utilizzati per la produzione della carta di identità elettronica, del documento di identità elettronico e della carta nazionale dei servizi, nonché le modalità di impiego.

7. Nel rispetto della disciplina generale fissata dai decreti di cui al presente articolo e delle vigenti disposizioni in materia di protezione dei dati personali, le pubbliche amministrazioni, nell'ambito dei rispettivi ordinamenti, possono sperimentare modalità di utilizzazione dei documenti di cui al presente articolo per l'erogazione di ulteriori servizi o utilità.

8. Le tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del decreto del Presidente della Repubblica 28 luglio 1967, n. 851, possono essere realizzate anche con modalità elettroniche e contenere le funzionalità della carta nazionale dei servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni.

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

Capo VI

SVILUPPO, ACQUISIZIONE E RIUSO DI SISTEMI INFORMATICI NELLE PUBBLICHE AMMINISTRAZIONI

Art. 67. Modalità di sviluppo ed acquisizione

1. Le pubbliche amministrazioni centrali, per i progetti finalizzati ad appalti di lavori e servizi ad alto contenuto di innovazione tecnologica, possono selezionare una o più proposte utilizzando il concorso di idee di cui all'articolo 57 del decreto del Presidente della Repubblica 21 dicembre 1999, n. 554.

2. Le amministrazioni appaltanti possono porre a base delle gare aventi ad oggetto la progettazione, o l'esecuzione, o entrambe, degli appalti di cui al comma 1, le proposte ideative acquisite ai sensi del comma 1, previo parere tecnico di congruità di DigitPA; alla relativa procedura è ammesso a partecipare, ai sensi dell'articolo 57, comma 6, del decreto del Presidente della Repubblica 21 dicembre 1999, n. 554, anche il soggetto selezionato ai sensi del comma 1, qualora sia in possesso dei relativi requisiti soggettivi.

Art. 68. Analisi comparativa delle soluzioni

1. Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei princìpi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:

a) software sviluppato per conto della pubblica amministrazione;

b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;

c) software libero o a codice sorgente aperto;

d) software fruibile in modalità cloud computing;

e) software di tipo proprietario mediante ricorso a licenza d'uso;

f) software combinazione delle precedenti soluzioni.

1-bis. A tal fine, le pubbliche amministrazioni prima di procedere all'acquisto, secondo le procedure di cui al codice di cui al decreto legislativo 12 aprile 2006 n. 163, effettuano una valutazione comparativa delle diverse soluzioni disponibili sulla base dei seguenti criteri:

a) costo complessivo del programma o soluzione quale costo di acquisto, di implementazione, di mantenimento e supporto;

b) livello di utilizzo di formati di dati e di interfacce di tipo aperto nonché di standard in grado di assicurare l'interoperabilità e la cooperazione applicativa tra i diversi sistemi informatici della pubblica amministrazione;

c) garanzie del fornitore in materia di livelli di sicurezza, conformità alla normativa in materia di protezione dei dati personali, livelli di servizio tenuto conto della tipologia di software acquisito. (235)

1-ter. Ove dalla valutazione comparativa di tipo tecnico ed economico, secondo i criteri di cui al comma 1-bis, risulti motivatamente l'impossibilità di accedere a soluzioni già disponibili all'interno della pubblica amministrazione, o a software liberi o a codici sorgente aperto, adeguati alle esigenze da soddisfare, è consentita l'acquisizione di programmi informatici di tipo proprietario mediante ricorso a licenza d'uso. La valutazione di cui al presente comma è effettuata secondo le modalità e i criteri definiti dall'Agenzia per l'Italia digitale, che, a richiesta di soggetti interessati, esprime altresì parere circa il loro rispetto. (235)

2. Le pubbliche amministrazioni nella predisposizione o nell'acquisizione dei programmi informatici, adottano soluzioni informatiche, quando possibile modulari, basate sui sistemi funzionali resi noti ai sensi dell'articolo 70, che assicurino l'interoperabilità e la cooperazione applicativa e consentano la rappresentazione dei dati e documenti in più formati, di cui almeno uno di tipo aperto, salvo che ricorrano motivate ed eccezionali esigenze.

2-bis. Le amministrazioni pubbliche comunicano tempestivamente a DigitPA l'adozione delle applicazioni informatiche e delle pratiche tecnologiche, e organizzative, adottate, fornendo ogni utile informazione ai fini della piena conoscibilità delle soluzioni adottate e dei risultati ottenuti, anche per favorire il riuso e la più ampia diffusione delle migliori pratiche.

3. Agli effetti del presente decreto legislativo si intende per:

a) formato dei dati di tipo aperto, un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi;

b) dati di tipo aperto, i dati che presentano le seguenti caratteristiche:

1) sono disponibili secondo i termini di una licenza che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato;

2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lettera a), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati;

3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione. L'Agenzia per l'Italia digitale deve stabilire, con propria deliberazione, i casi eccezionali, individuati secondo criteri oggettivi, trasparenti e verificabili, in cui essi sono resi disponibili a tariffe superiori ai costi marginali. In ogni caso, l'Agenzia, nel trattamento dei casi eccezionali individuati, si attiene alle indicazioni fornite dalla direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, sul riutilizzo dell'informazione del settore pubblico, recepita con il decreto legislativo 24 gennaio 2006, n. 36.

4. DigitPA istruisce ed aggiorna, con periodicità almeno annuale, un repertorio dei formati aperti utilizzabili nelle pubbliche amministrazioni e delle modalità di trasferimento dei formati.

Art. 69. Riuso dei programmi informatici

1. Le pubbliche amministrazioni che siano titolari di programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno obbligo di darli in formato sorgente, completi della documentazione disponibile, in uso gratuito ad altre pubbliche amministrazioni che li richiedono e che intendano adattarli alle proprie esigenze, salvo motivate ragioni.

2. Al fine di favorire il riuso dei programmi informatici di proprietà delle pubbliche amministrazioni, ai sensi del comma 1, nei capitolati o nelle specifiche di progetto è previsto ove possibile, che i programmi appositamente sviluppati per conto e a spese dell'amministrazione siano facilmente portabili su altre piattaforme e conformi alla definizione e regolamentazione effettuata da DigitPA, ai sensi dell'articolo 68, comma 2.

3. Le pubbliche amministrazioni inseriscono, nei contratti per l'acquisizione di programmi informatici o di singoli moduli, di cui al comma 1, clausole che garantiscano il diritto di disporre dei programmi ai fini del riuso da parte della medesima o di altre amministrazioni.

4. Nei contratti di acquisizione di programmi informatici sviluppati per conto e a spese delle amministrazioni, le stesse possono includere clausole, concordate con il fornitore,

che tengano conto delle caratteristiche economiche ed organizzative di quest'ultimo, volte a vincolarlo, per un determinato lasso di tempo, a fornire, su richiesta di altre amministrazioni, servizi che consentono il riuso dei programmi o dei singoli moduli. Le clausole suddette definiscono le condizioni da osservare per la prestazione dei servizi indicati.