

Disposizioni in materia di documentazione amministrativa

- *d.P.R. n.445 del 28.12.2000, T.U. delle norme in materia di documentazione amministrativa*
- *d.Lgs. n.82 del 7 marzo 2005, Codice dell'Amministrazione Digitale (CAD)*

ovvero della semplificazione ...



Scopo della Semplificazione amministrativa

Passare dalla cultura della sudditanza e del sospetto ...
alla cultura della fiducia e della collaborazione, eliminando le
file agli sportelli, i lunghi tempi d'attesa, ricorrendo alle
autocertificazioni e all'impiego delle risorse telematiche:

- **Autocertificazioni al posto dei certificati**
- **Informatizzazione dei processi e dei documenti**
- **Termini certi per concludere le procedure**
- **Testi Unici al posto di centinaia di leggi e regolamenti**
- **... ecc. ecc. ecc.**

Gli antenati della semplificazione

Anno 1968 - legge n.15

- Le importanti novità che la legge conteneva non sono state applicate
- le novità sono rimaste sconosciute alla P.A., ai cittadini, alle imprese in quanto mancava un'adeguata cultura amministrativa pronta a recepire il nuovo

Anno 1990 - legge 142 e legge 241

Anno 1997 - legge 127

Anno 1998 - legge 191, d.P.R. 403

Di che cosa tratta il Testo Unico 445/2000 ?

1. Tutte le norme relative alla presentazione delle istanze alla P.A. e ai soggetti equiparati.
2. Tutte le norme che prevedono attività di autenticazione e legalizzazione da parte di organi della P.A.
3. Delle norme sul documento informatico, sulla firma elettronica e sulla carta d'identità elettronica
4. Del protocollo elettronico

Art.1 - Definizioni

L'art.1 propone tutte le definizioni delle singole fattispecie, di particolare interesse sono le definizioni relative alla differenza tra documento d'identità e documento di riconoscimento

Pubblico Ufficiale

- Notaio,
- Cancelliere di tribunale,
- Segretario comunale,
- Funzionario incaricato dal Sindaco.

Documento di riconoscimento e Documento d'identità

DOCUMENTO DI RICONOSCIMENTO: Ogni documento munito di fotografia del titolare e rilasciato, su supporto magnetico, cartaceo o informatico, da una P.A. italiana o di altri Stati, che consente l'identificazione personale del titolare (*tessere di viaggio, tessere ministeriali o delle forze armate e di polizia, patenti di guida, patenti nautiche, libretti di pensione, porto d'armi, ecc.*);

DOCUMENTO D'IDENTITÀ': La carta d'identità ed ogni altro documento munito di fotografia rilasciato su supporto cartaceo, magnetico o informatico, dall'Amministrazione competente dello Stato Italiano o di altri Stati, con la finalità prevalente di dimostrare l'identità personale suo titolare. (*passaporto, documento di autorizzazione per l'espatrio dei minori*)

Art.2 – Oggetto della Legge

- Pubbliche Amministrazioni;
- Gestori di Pubblici Servizi: es. HERA, ENEL, TELECOM, Poste Italiane (*non Bancoposta*), SETA, Ferrovie., ecc.;
- soggetti privati che vi consentono.

P.A. e Uffici Giudiziari

L'art.2 obbliga **TUTTI gli uffici della P.A.** e dei **gestori dei pubblici servizi** ad avvalersi delle norme sulla semplificazione.

Tra le P.A. **non** sono da intendersi gli **Uffici Giudiziari** quando esplicano attività di tipo giurisdizionale. Per tali uffici le norme in materia di documentazione amministrativa si applicano nei seguenti casi:

- quando si tratti di procedimenti **strettamente amministrativi** (gestione del personale, attività negoziali)
- nel caso di attività di natura **sostanzialmente amministrativa** pur connesse all'esercizio della funzione giurisdizionale (iscrizione delle cause a ruolo, iscrizione all'albo dei consulenti tecnici, gratuito patrocinio)
- nell'ambito delle attività poste in essere dal personale delle cancellerie e segreterie giudiziarie **avente natura non giurisdizionale** (atti notori, rinuncia all'eredità, accettazione dell'eredità con beneficio di inventario).

Art.3 - Soggetti della legge

- Cittadini e persone giuridiche pubbliche o private che hanno **sede legale nei paesi della U.E.**;
- Cittadini **extracomunitari residenti o soggiornanti** in Italia, possono utilizzare l'autocertificazione o le dichiarazioni sostitutive limitatamente alle situazioni certificabili dalla P.A. italiana, fatte salve le speciali disposizioni concernenti la disciplina dell'immigrazione e la condizione dello straniero, o qualora vi siano convenzioni internazionali fra l'Italia e il Paese di provenienza del dichiarante.
- Al di fuori di tali casi le situazioni personali sono documentabili mediante certificati o attestazioni **rilasciati dalla competente autorità straniera, corredati di traduzione in lingua italiana autenticata dall'autorità consolare italiana**

Cittadini U.E. e non U.E. (stranieri)

- Le misure di semplificazione possono essere utilizzate anche da **persone giuridiche o Enti aventi sede nell'U.E.**
- I cittadini Extra U.E. possono utilizzare gli strumenti della semplificazione **anche se solo soggiornanti** e non residenti.
- i documenti tradotti dalla lingua originale **devono essere legalizzati dall'autorità consolare italiana all'estero e non più dall'autorità consolare straniera in Italia.**

Ingresso e soggiorno dei cittadini extracomunitari

Tutti i cittadini extracomunitari possono entrare in Italia solo se in possesso del passaporto e del **visto d'ingresso** (*salvo i casi di esenzione*).

Ai cittadini extracomunitari che si trattengono per un periodo superiore agli 8 giorni, deve essere rilasciato il **permesso di soggiorno**.

La **carta di soggiorno** può essere rilasciata ai cittadini extra U.E. dopo almeno 4 anni di residenza.

I cittadini extracomunitari possono soggiornare in Italia anche se in possesso di un **permesso di soggiorno rilasciato da un Paese dell'U.E.**

Art.4 - Impedimento alla sottoscrizione

Chi non può firmare per impedimento fisico può rilasciare dichiarazione al Pubblico Ufficiale, che attesta che la dichiarazione è stata a lui resa

Chi non può rilasciare dichiarazioni a causa di un impedimento “**temporaneo**” per motivi di salute, la dichiarazione può essere resa dal coniuge o dai figli o da parenti fino al 3° grado (nonni, nipoti, bisnonni, pronipoti, fratelli, zii), al Pubblico ufficiale

Tali dichiarazioni non possono riguardare le esenzioni fiscali

Art.18 - Copie autentiche, chi le fa?

Pubblico Ufficiale;

L'Ufficio Pubblico che ha **emesso l'atto** o che ha in **deposito l'atto originale** (*non vi è necessità di alcun incarico specifico*);

Per atti da consegnare alla P.A.: **responsabile del procedimento** o chi **riceve materialmente la documentazione** (*non vi è necessità di alcun incarico specifico*), e senza obbligo di deposito dell'originale presso l'Amministrazione precedente.

Art.18 - Copie autentiche, come si fa?

Apponendo sulla copia dell'originale apposito timbro o dicitura riportante i richiami normativi, il numero di fogli da cui è composto l'originale, il luogo e la data del rilascio, il timbro dell'Ente, il nome di chi effettua l'autentica e la sua firma per esteso;

Se la copia è composta da più fogli, la **firma per esteso** di chi autentica deve essere riportata su tutti i fogli.

Art.19 - Modalità alternative all'autentica di copie

Con **dichiarazione sostitutiva di atto di notorietà**,
limitatamente a:

- *documenti tenuti o rilasciati dalla P.A.;*
- *pubblicazioni, titoli di studio e servizio;*
- *documenti fiscali che debbano essere conservati da privati.*

Art.21 - Autentica delle firme

L'autentica di firme per istanze o dichiarazioni sostitutive rivolte alla P.A. o a gestori di pubblici servizi **NON ESISTE PIU'**, se non per riscossione da parte di terzi di benefici economici, o nei casi previste dalle norme:

- dichiarazione di vendita di beni mobili registrati (auto e moto veicoli, imbarcazioni);
- quietanze liberatorie;
- procedimenti elettorali;
- adozione internazionale (*limitatamente alle dichiarazioni di consenso all'incontro tra gli aspiranti all'adozione ed il minore da adottare, proposto dall'autorità straniera, da parte degli aspiranti all'adozione*);

L'autentica di firma esiste solo per istanze o dichiarazioni sostitutive rivolte a soggetti **privati**, e sono eseguite dai Pubblici Ufficiali.

In tali casi l'autentica è redatta di seguito alla sottoscrizione e il pubblico ufficiale attesta che la firma è stata posta in sua presenza, previo accertamento dell'identità del dichiarante, indicando le modalità di detta identificazione

Quando si autentica la firma ?

TIPOLOGIA DI ATTI	AUTENTICA
Istanze e dichiarazioni sostitutive inviate a organi della P.A.	Art. 38 c.3 NON PUO' ESSERE RICHIESTA ED EFFETTUATA
Istanze e dichiarazioni sostitutive inviate a soggetti diversi dalla P.A.	Art.21 c.2 I PRIVATI POSSONO RICHIEDERLA E ACCETTARLA
Istanze e dichiarazioni sostitutive inviate alla P.A. o a soggetti privati al fine della riscossione da parte di terzi di benefici economici	Art.21 c.2 E' SEMPRE NECESSARIA

Art.33 - Atti in lingua straniera

Atti presentati alla P.A. possono essere accettati se **tradotti in lingua italiana**, certificata conforme all'originale dal competente consolato o da un traduttore ufficiale;

le firme di pubblici ufficiali stranieri devono essere **legalizzate** (se provenienti dall'estero dall'autorità consolare italiana all'estero, se provenienti da consolati stranieri in Italia dalla Prefettura). La legalizzazione può essere esclusa o sostituita da altre forme di verifica, sulla base di appositi accordi internazionali (ex.: apostille).

Legalizzazione di firma

E' l'attestazione ufficiale della **legale qualità** di chi ha apposto la **firma su atti pubblici**

E' effettuata sui documenti della P.A. che devono aver valore anche all'estero, e di norma viene eseguita dalla **Prefettura**, dove esiste apposito ufficio.

La legalizzazione della firma può essere eseguita esclusivamente se questa è stata precedentemente depositata presso l'organo competente ad effettuare la legalizzazione.

Chi effettua la legalizzazione di firma

Documenti redatti in Italia da valere per l'estero	Legalizzati dal Ministero competente o suoi organi periferici (per i Comuni è la Prefettura)
Documenti redatti all'estero da autorità estere	Legalizzate dal Consolato o Ambasciata Italiana all'estero (o Apostille dell'autorità straniera)
Documenti redatti all'estero da consolati o ambasciate italiani	NON VANNO LEGALIZZATI
Documenti redatti in Italia da consolati o ambasciate estere	Vanno legalizzate da qualsiasi Prefettura (... quasi)

Art.34 - Legalizzazione di fotografie

Le fotografie possono essere legalizzate (autenticate) solo se devono essere utilizzate per il **rilascio di un documento d'identità personale**.

La legalizzazione è eseguita da chi rilascia il documento d'identità o dal dipendente incaricato dal Sindaco.

Art.35 - Documenti d'identità

Nella normativa per la semplificazione amministrativa **documento d'identità e di riconoscimento hanno lo stesso valore**, ovvero sono fra di loro equipollenti: carta d'identità, passaporto, patente di guida, libretto di pensione, porto d'armi, **tutte** le tessere di riconoscimento munite di foto e rilasciate da una PA.

Nel caso in cui il documento fosse **scaduto**, i dati in esso contenuto devono essere considerati validi se l'interessato dichiara che i dati stessi non sono variati rispetto alla data di rilascio.

Art.38 - Sottoscrizione e invio di istanze e dichiarazioni sostitutive

Istanze e dichiarazioni dirette alla P.A. possono alternativamente essere:

- sottoscritte **davanti** al dipendente addetto a riceverle;
- presentate unitamente alla **fotocopia di un documento d'identità** dell'interessato, adottando tale modalità possono essere anche inviate tramite posta ordinaria o strumenti informatici.

*“L'allegazione della copia fotostatica del documento del sottoscrittore della dichiarazione sostitutiva, prescritta dal c.3 dell'art. 38 d.P.R. n. 445/20000, è **adempimento inderogabile**, atto a conferire, in considerazione della sua introduzione come forma di semplificazione, legale autenticità alla sottoscrizione apposta in calce alla dichiarazione e giuridica esistenza ed efficacia all'autocertificazione (sic), trattandosi di un elemento integrante della fattispecie normativa, teso a stabilire, data l'unità della fotocopia sostitutiva del documento di identità e della dichiarazione sostitutiva, **un collegamento tra la dichiarazione ed il documento ed a comprovare**, oltre alle generalità del dichiarante, l'imputabilità soggettiva della dichiarazione al soggetto che la presta”* (ex, Consiglio di Stato sez.V: 26/03/2012, n. 1739; Cons. St. Sez. VI, 2.5.2011, n. 2579; 4.6.2009, n.3442; Sez. V, 7.11.2007, n. 5761; 11.5.2007, n. 2333).

*“La giurisprudenza di questo Consiglio di Stato è concorde nell’affermare che, in presenza di un’espressa prescrizione, contenuta nella lex specialis di gara e posta a pena di esclusione, di allegare all’offerta economica copia del documento di identità dei sottoscrittori, è legittima l’esclusione pronunciata per mancata presentazione della copia del documento di identità; ...; ne’ la stessa prescrizione si risolve in un **mero formalismo**, perchè è diretta a ricondurre incontrovertibilmente al suo autore la sottoscrizione della più importante delle dichiarazioni di volontà che intervengono nella procedura concorsuale; infine, la clausola non può ritenersi ne’ illogica ne’ sproporzionata, perchè trova la sua ragion d’essere nell’esigenza di soddisfare un interesse apprezzabile dell’amministrazione, **dando certezza in ordine alla provenienza della dichiarazione**, e nel contempo si limita ad imporre ai partecipanti uno sforzo minimo, proporzionato rispetto all’interesse pubblico perseguito” (Cons. St. sentenza 2012, cfr. Cons. St., sez. VI, 24/01/2011 n. 478 e 27/04/2011 n. 2478, nonchè sez. V, 23/11/2010 n. 8151).*

Art.41 - Validità dei documenti

Validità **illimitata** per i documenti non soggetti a modifiche (certificati di stato civile);

Validità di **6 mesi** per tutti gli altri.

Certificati ed estratti di stato civile

I **certificati** di stato civile (nascita, morte, matrimonio/unione civile), contengono **solo i dati essenziali** riportati sull'atto: generalità, estremi dell'atto, data e luogo dell'evento.

Gli **estratti**, oltre a tali dati, contengono le **modifiche o integrazioni** (*annotazioni*), avvenute successivamente alla formazione dell'atto (ex.: divorzio, separazione dei beni, morte)

Art.43 - Acquisizione d'ufficio

Le P.A. **NON** possono chiedere all'interessato atti o documenti autocertificabili (unica eccezione i Tribunali o nel caso norme specifiche lo prevedessero), ma devono **acquisire d'ufficio tale documentazione** previa **indicazione, da parte dell'interessato, dell'Amministrazione procedente, o accettare l'autocertificazione.**

L'acquisizione diretta di tali documenti può avvenire per via **informatica, anche con modalità diverse da quelle del certificato**, pur nella certezza della provenienza, **senza che sia necessario il successivo invio dell'originale.**

L'articolo 14 d.L. n. 69/2013 "*Misure per favorire la diffusione del domicilio digitale*" ha stabilito che, ai fini della verifica della provenienza delle comunicazioni, è ***in ogni caso esclusa la trasmissione di documenti a mezzo fax***, tra P.A.

L'art. 15 legge 183/2011

Dal 1° gennaio 2012 è in vigore l'art. 15 legge 12.11.2011 n. 183, contenente modifiche al D.P.R. 445/2000.

Tale normativa è diretta “... *alla completa semplificazione in materia di certificazione nei rapporti tra P.A. e privati con l'obbligo di acquisizione diretta di dati presso le amministrazioni certificanti da parte delle amministrazioni procedenti e, in alternativa, la produzione da parte degli interessati solo di dichiarazioni sostitutive di certificazioni o dell'atto di notorietà*”.

Le P.A., e i gestori di pubblici servizi, **non possono più richiedere all'utenza privata atti o certificati contenenti informazioni già in possesso della P.A..**

Le certificazioni rilasciate dalle P.A. in ordine a stati, qualità personali e fatti **sono valide e utilizzabili solo nei rapporti tra privati;**

Nei rapporti con gli organi della P.A. e i gestori di pubblici servizi **i certificati sono sempre sostituiti dalle dichiarazioni sostitutive** di certificazione o dall'atto di notorietà

A far data del 1 gennaio 2012 sui certificati rilasciati dalle P.A. deve essere apposta, a pena di nullità, la dicitura ***“il presente certificato non può essere prodotto agli organi della PA o ai privati gestori di pubblici servizi”***

Oltre alla **nullità della certificazione** in assenza della prescritta dicitura, la mancata applicazione della normativa in materia comporta **violazione, in caso di richiesta o accettazione dei certificati, dei doveri d'ufficio** ex articolo 74, comma 2, lett a) del DPR 445/2000.

Art.45 - Documentazione mediante esibizione di un documento d'identità

E' fatto **DIVIETO** alla P.A., nel caso in cui all'atto della presentazione di un'istanza sia richiesta l'esibizione di un documento d'identità o riconoscimento, di richiedere documenti attestanti stati o fatti contenuti nel documento stesso, anche se scaduto se l'interessato dichiara in modo scritto che i dati sono ancora validi

L'esibizione di un documento d'identità a un soggetto pubblico, a seconda dei dati che contiene, **sostituisce i certificati di nascita, residenza, cittadinanza e stato civile.**

Il documento in questione deve essere fotocopiato e allegato agli atti dell'istruttoria.

Art.46 - Autocertificazione

Tutti i certificati o documenti rilasciati dalla P.A. (ad eccezione di quelli per cui esiste un espresso divieto) sono **autocertificabili**.

Atti che non possono essere autocertificati:

- Certificati medici, sanitari, veterinari;
- di origine;
- di conformità CEE;
- di marchi o brevetti.

L'autocertificazione **NON** necessita di autentica o di fotocopia di documento d'identità ed è **gratuita**.

Le P.A. **sono tenute** a fornire i moduli pre-stampati per facilitarne l'utilizzo.

Un dettaglio rilevante ma spesso trascurato riguarda il fatto che con l'autocertificazione deve **corrispondere al certificato** a cui fa riferimento nel momento in cui viene sottoscritta, e non alla reale situazione dei fatti a quel momento.

Art.47 - Dichiarazioni sostitutive di atto di notorietà

Stati, fatti e qualità personali, possono essere comprovati con dichiarazioni sostitutive di atto di notorietà che, se dirette a P.A., **NON DEVONO** essere autenticate e sono **gratuite**. Sono gratuite anche quelle dirette a soggetti privati, ma nel caso in cui debba essere effettuata l'autentica della sottoscrizione, questa è soggetta al pagamento delle imposte di legge e dei diritti di segreteria.

Tali dichiarazioni possono riguardare anche stati, fatti e qualità di **altre persone** di cui il dichiarante abbia diretta conoscenza.

Le dichiarazioni hanno la stessa validità temporale degli atti che sostituiscono.

Stati, fatti e qualità personali fatti oggetto di dichiarazione sostitutiva di atto di notorietà

1. Tutti quelli che **non sono autocertificabili**, ma possono essere dichiarati anche dati autocertificabili;
2. Tutti quelli riguardanti terze persone, ma a **diretta conoscenza dell'interessato**;
3. Lo smarrimento del documento di riconoscimento (non d'identità) o attestante stati, fatti e qualità personali;
4. La conformità all'originale di una copia;
5. Può essere resa da coniuge o dai parenti entro il 3° grado, della persona temporaneamente impedita.

Tutto così semplice? ... Mica tanto

La **circolare del Ministero dell'Interno n.10/1993**, pur facendo riferimento alla L.n.15/1968, è ritenuta tutt'ora applicabile anche al d.P.R. 445/2000, afferma che:

“... *tra le autentiche di sottoscrizioni da effettuarsi ai sensi dell'art.20 della L. n. 15/1968 [ora artt.21 e 47 d.P.R. 445/2000], rientrano anche quelle **dichiarazioni di impegno** richieste per la partecipazione ad un concorso od al fine di ottenere, più genericamente, un **determinato provvedimento** da una PA. Al contrario si conferma che rimangono escluse tutte quelle manifestazioni di volontà di carattere «**negoziale**» intercorrenti fra privati ovvero inerenti rapporti privatistici quali ad esempio le accettazioni, rinunce di incarichi o le procure.”*

A quest'ultimo riguardo occorre fare un'ulteriore precisazione. La procura è lo strumento giuridico attraverso il quale si realizza l'istituto, tipico del diritto privato, della **rappresentanza**, in virtù del quale un soggetto è autorizzato per legge a «**sostituirsi ad altro soggetto** nel compimento di attività giuridica per conto di quest'ultimo». Il rappresentante, quindi, partecipa al compimento di attività giuridica e ciò lo differenzia nettamente dal delegato.

Il delegato, infatti, nella fattispecie più ricorrenti nei rapporti con la propria volontà con la P.A. quali: ritiro di documenti, riscossioni di pensioni, è **semplicemente colui che riceve l'estrinsecazione materiale di un provvedimento amministrativo che si è già perfezionato**.

Pertanto, ..., **gli atti di delega, sempreché diretti ad una PA e non concretanti una procura**, attesa la succitata differenziazione, rientrano tra gli atti di cui è **possibile autenticare la sottoscrizione ai sensi dell'art.20 L.n.15/1968.**³⁵

Dichiarazioni sostitutive - schema comparativo

Di certificazione (art.46)	Di atto di notorietà (art.47)
E' sufficiente la dichiarazione sottoscritta dall'interessato	La sola sottoscrizione dell'interessato non è sufficiente
Deve riguardare un documento o certificato rilasciato dalla P.A.	Deve riguardare qualsiasi stato, fatto o qualità personale a diretta conoscenza dell'interessato
Non serve alcuna modalità di autentica di firma	La firma va comprovata o autenticata con i mezzi di cui agli artt.21 e 38

Struttura delle autocertificazioni e delle dichiarazioni sostitutive

1. Amministrazione a cui è diretto il documento
2. procedura per la quale deve essere utilizzato il documento
3. dati anagrafici del dichiarante e indirizzo;
4. dichiarazione del dichiarante di essere a conoscenza delle conseguenze penali derivanti da dichiarazioni false;
5. luogo e data della sottoscrizione;
6. firma del dichiarante;
7. modalità con cui il documento può essere comunicato o inviato all'Amministrazione procedente;
8. informativa privacy.

Il sistema dei controlli e sue finalità. Obbligatorietà

Il T.U. sulla documentazione amministrativa raccoglie e coordina le numerose disposizioni normative previgenti in materia di semplificazione amministrativa, operando una precisa scelta a favore del principio di semplificazione, **senza, con ciò, recare pregiudizio al principio di certezza**. Infatti la semplificazione deve essere considerata come strumento più diretto ed immediato per il perseguimento della certezza pubblica.

Proprio per coniugare la prima (semplificazione) con la seconda esigenza (certezza) il T. U. ha dettato alcune importanti disposizioni, che da un lato confermano **l'obbligatorietà del controllo sulle dichiarazioni sostitutive**, già sancita dal D.P.R. 403/1998 e, dall'altro, disciplinano le diverse responsabilità ed le conseguenti sanzioni per le dichiarazioni mendaci.

Nel sistema di produzione e circolazione delle certezze pubbliche tramite autocertificazioni, sia la PA che i cittadini svolgono un ruolo specifico dal quale conseguono precise responsabilità.

Infatti, l'amministrazione, attraverso il controllo di quanto dichiarato e la possibilità di far valere la responsabilità del dichiarante, è chiamata ad assicurare la presenza delle condizioni necessarie per garantire ai soggetti dell'ordinamento la plausibilità della rispondenza al vero di quanto viene dichiarato dagli interessati. Gli interessati, d'altra parte, sono chiamati sia a contribuire, con una propria assunzione di responsabilità, alla semplificazione degli adempimenti necessari per assicurare la certezza pubblica, sia a fornire, in virtù del proprio interesse a non incorrere in sanzioni, delle garanzie in merito alla attendibilità del sistema delle certezze pubbliche..

In conclusione, è possibile affermare che il sistema dei controlli svolge una funzione di **garanzia della certezza pubblica**.

La veridicità delle dichiarazioni: l'inversione dell'onere della prova dal cittadino alla PA

L'estensione dell'istituto delle autocertificazioni e delle dichiarazioni sostitutive dei certificati amministrativi non solleva le amministrazioni dall'effettuare i controlli rispetto alla veridicità delle dichiarazioni.

Le certificazioni, infatti, sono richieste come elemento probatorio per verificare l'effettivo possesso di requisiti previsti dalle leggi, o l'assenza di cause ostative, perché il cittadino possa beneficiare di un provvedimento a sé favorevole.

Pertanto, la PA deve verificare, dal punto di vista sostanziale, che la dichiarazione sostitutiva **corrisponda all'effettivo possesso dei requisiti.**

La semplificazione, però, dà luogo ad una sorta di **inversione di onere della prova.** Nel precedente regime era il cittadino a dover fornire la prova, attestata dalle certificazioni amministrative che doveva procurarsi personalmente.

Nell'attuale regime, invece, è la PA che, acquisita una dichiarazione sostitutiva di certificazione da parte del cittadino, deve curarsi di provare che essa sia eventualmente falsa.

Si ha, pertanto, implicitamente una **presunzione di veridicità della dichiarazione del cittadino** ed una modifica del ruolo delle amministrazioni certificanti, le quali non erogano servizi ai cittadini, ma, al contrario, alle amministrazioni procedenti, rispetto alle quali si pongono come servizi di staff che erogano prestazioni intermedie

La natura dei controlli

Le previsioni in materia di controllo sono state contenute negli **articoli 71 e 72** del d.P.R. 445/2000.

Tali disposizioni non specificano le modalità con cui vengono effettuati i controlli, in quanto non possono essere definite in modo univoco per tutte le PA: le modalità di controllo **vanno commisurate alle dimensioni ed alle caratteristiche organizzative delle singole amministrazioni** chiamate ad operare il controllo.

In merito alla *natura giuridica* del controllo sulle autocertificazioni, esso si configura come un **subprocedimento eventuale**, che si colloca nel procedimento per il quale viene presentata la dichiarazione sostitutiva. Esso va, dunque, ricollegato alla disciplina del procedimento principale: in ogni caso sarà sufficiente comunicare agli interessati solo l'avvio di quest'ultimo, poiché sia la presentazione delle dichiarazioni sostitutive, sia il controllo su di esse possono essere considerati come eventualità riconducibili alla stessa.

Il beneficio concesso **decade** se dal controllo effettuato risulta che le dichiarazioni non siano corrispondenti al vero: da ciò si evince che l'attività di controllo non debba necessariamente essere esaurita prima dell'adozione del provvedimento finale

Art.71 - Modalità dei controlli da parte di Enti Pubblici

Ai sensi dell'art. 71, le amministrazioni procedenti sono tenute ad effettuare idonei controlli sulle dichiarazioni sostitutive di cui agli articoli 46 e 47. Tale articolo dispone un **comportamento obbligatorio e cogente**: pertanto si tratta di un dovere d'ufficio, che completa l'*iter* procedimentale anche se il controllo interviene dopo che il provvedimento sia già stato emanato.

L'autodichiarazione costituisce **valido elemento e presupposto, condizione necessaria e sufficiente** per l'emanazione del provvedimento. Tuttavia la fiducia che la legislazione concede al cittadino, non è assoluta, e la PA deve procedere ai riscontri necessari..

I controlli debbono essere fatti:

- 1. in modo puntuale;**
- 2. a campione;**
- 3. nei casi in cui vi siano fondati dubbi sulla veridicità delle dichiarazioni.**

Il controllo consiste nella verifica di quanto dichiarato sulla documentazione in possesso della P.A. o presso i privati in grado di fornire notizie certe su quanto dichiarato.

La risposta alle richieste di controllo inoltrate alla P.A. devono essere data entro **30 gg.** (art.72).

La dottrina ha, poi, evidenziato che il T.U. non limita i mezzi di controllo alle verifiche cartolari, ma lascia aperta la possibilità di ulteriori interventi dell'amministrazione procedente che, in caso di impossibilità di verifica documentale, si estendono ad altri mezzi di accertamento, quali ad esempio audizioni di testimoni, ispezioni etc., eventualmente avvalendosi anche dell'intervento dell'autorità di polizia competente

Adempimenti preliminari e modalità di effettuazione dei controlli

Le PA possono definire le modalità di controllo più idonee alla propria realtà operativa. Sono, tuttavia, necessari degli adempimenti che possono accomunare più amministrazioni.

Tali **adempimenti** possono essere:

1. **a carattere generale**: le amministrazioni devono, infatti, definire i canali di scambio dei propri dati e formulare protocolli d'intesa con altre amministrazioni interessate a tale scambio;
2. **a carattere specifico**: le amministrazioni devono individuare le linee guida per lo svolgimento dell'attività di controllo, diversa per ciascun tipo di procedimento, e comunicarle agli uffici adibiti al controllo; devono, inoltre, individuare le aree di attività in cui il rischio di dichiarazioni mendaci è maggiore.

Generalmente i controlli possono essere disposti in due diverse ed alternative **modalità** (cfr. art. 71, comma 2, D.P.R. 445/2000):

1. attraverso la **consultazione diretta degli archivi** dell'amministrazione certificante, per la quale è necessario, però, che vi sia un'interconnessione tra le varie amministrazioni;
2. attraverso la **richiesta all'amministrazione certificante** di una conferma scritta, comunicabile anche con strumenti telematici e informatici, della corrispondenza di quanto dichiarato con le risultanze dei registri da essa custoditi.

In particolare, l'acquisizione diretta della documentazione mediante consultazione degli archivi dell'amministrazione certificante avviene:

- in base a un'**autorizzazione** con la quale l'amministrazione certificante indica a quella precedente i **limiti e le condizioni** di accesso ai propri archivi, al fine di salvaguardare la riservatezza dei dati personali;
- nel rispetto del **divieto**, per l'amministrazione precedente, di **accedere a dati diversi da quelli dei quali è necessario procedere alla verifica**;
- utilizzando il sistema del canale **telematico**;
- nel rispetto dell'obbligo, per le amministrazioni certificanti, di consentire, **gratuitamente**, la consultazione telematica dei propri archivi informatici.

Controlli mirati o puntuali

Sono controlli che devono essere fatti ogni qual volta debba essere **emanato un provvedimento favorevole** in seguito a:

- ➔ *procedimenti concorsuali;*
- ➔ *appalti e/o gare;*
- ➔ *rilascio di licenze, concessioni ed autorizzazioni in settori nei quali le informazioni rese costituiscono discriminante per il provvedimento finale.*

Controlli a campione

E' un controllo effettuato su un numero predeterminato di dichiarazioni.

Il campione deve essere **significativo** sia come livello quantitativo, sia in relazione all'idoneità a rivelare lo stato complessivo delle procedure.

controlli per “fondato dubbio”

Il dubbio è fondato se si basa su un fatto **incompatibile con l'autocertificazione** (ad es.: dati che contrastano con altri dati in possesso dell'Amministrazione o già dichiarati in precedenza), e non per un dubbio generico del dipendente pubblico.

Le irregolarità e le omissioni nelle dichiarazioni sostitutive

L'articolo 71, comma 3, d.P.R. 445/2000 prende in considerazione l'ipotesi in cui siano rilevabili d'ufficio irregolarità od omissioni nelle dichiarazioni sostitutive, che però non costituiscano falsità.

L'**irregolarità** consiste nell'esistenza di un vizio nella dichiarazione che non ne comporti la nullità, ma consenta ugualmente di utilizzare la dichiarazione medesima, ai fini procedurali, attraverso una semplice rettifica.

L'**omissione** consiste, invece, nell'incompletezza della dichiarazione, che ometta una parte di quanto è finalizzata ad attestare.

Il principio generale è che se dietro a queste irregolarità od omissioni **non v'è l'intenzione fraudolenta** di falsificare la realtà di quanto dichiarato, **occorre dare comunque corso al procedimento**.

Tale principio porta ad una serie di conseguenze. In primo luogo, l'irregolarità non genera decadenze a carico del dichiarante, il quale conserva il diritto a che l'amministrazione completi l'istruttoria e si pronunci motivatamente e con il provvedimento finale espresso.

La **rilevazione d'ufficio** dell'irregolarità o dell'omissione fa scattare l'obbligo, a carico del funzionario competente a ricevere la documentazione (o del responsabile del procedimento), **di informare tempestivamente il cittadino di tali irregolarità**, per invitarlo a perfezionare la dichiarazione. Il soggetto interessato è tenuto, obbligato a regolarizzare o completare la dichiarazione. Questo obbligo non è sanzionato da decadenze. Tuttavia, **finché non sia provveduto alla regolarizzazione, il procedimento resta sospeso**. (art. 71, comma 3).

Le responsabilità dei soggetti dichiaranti

Gli artt. 75 e 76 del D.P.R. 445/2000 stabiliscono le **sanzioni** a carico di coloro i quali presentino dichiarazioni mendaci. Queste possono essere procedurali e penali.

L'art. 75 si riferisce alla prima fattispecie e disciplina la **decadenza dai benefici** ottenuti dall'emanazione di un provvedimento favorevole in base ad una dichiarazione falsa. In tal caso, ferme restando le sanzioni penali di cui all'articolo 76, qualora dal controllo di cui all'articolo 71 emerga la **non veridicità del contenuto della dichiarazione**, il dichiarante decade dai benefici eventualmente conseguenti al provvedimento emanato sulla base della dichiarazione non veritiera.

Dunque, accertata la falsità delle dichiarazioni, l'amministrazione pubblica procedente comunica al richiedente la decadenza dai benefici e provvede di conseguenza, riformulando la graduatoria, chiedendo indietro eventuali erogazioni economiche, anche coattivamente, procedendo alle denunce per i reati previsti dalla legge.

L'art. 76, invece, disciplina le *sanzioni di natura penale*. Il comma 1 prevede che chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal Testo Unico è **punito ai sensi del codice penale** e delle leggi speciali in materia.

I privati possono incorrere nelle seguenti *fattispecie incriminanti*:

- **falsa attestazione o dichiarazione a un pubblico ufficiale sulla identità o su qualità personali proprie o di altri** (art. 495 c.p.): è commesso da chiunque dichiara o attesta falsamente al pubblico ufficiale, in un atto pubblico, l'identità o lo stato o le altre qualità della propria o dell'altrui persona;
- **false dichiarazioni sull'identità o su qualità personali, proprie o altrui** (art. 496 c.p.): commette tale reato chiunque, interrogato sull'identità, sullo stato o su altre qualità della propria o dell'altrui persona, fa mendaci dichiarazioni a un pubblico ufficiale o a persona incaricata di un pubblico servizio;
- **falsità materiale commessa dal privato** (art. 482 c.p.): tale reato estende ai cittadini privati i reati di falso previsti a carico dei pubblici ufficiali dagli articoli 476, 477 e 478 del codice penale, riducendo le pene di un terzo. Le ipotesi di falso sono la falsità materiale e la falsità ideologica;
- **uso di atto falso** (art. 489 c.p.): è il reato commesso da chi, pur non avendo compiuto l'atto o la dichiarazione falsa, faccia uso di un atto falso;

La responsabilità in materia di accertamento d'ufficio e di esecuzione dei controlli

L'art. 72 del d.P.R. 445/2000 prevede che, ai fini dell'accertamento d'ufficio dei controlli di cui all'articolo 71 e della predisposizione delle convenzioni quadro, le amministrazioni certificanti sono tenute ad individuare un **ufficio responsabile** per tutte le attività volte a gestire, garantire e verificare la trasmissione dei dati o l'accesso diretto agli stessi da parte delle amministrazioni procedenti.

Attraverso tale ufficio, le amministrazioni certificanti individuano e rendono note, mediante la pubblicazione sul sito istituzionale dell'amministrazione, le ***misure organizzative*** adottate per l'efficiente, efficace e tempestiva acquisizione d'ufficio dei dati e per l'effettuazione dei controlli medesimi, nonché le modalità per la loro esecuzione.

È poi importante evidenziare come la disposizione in esami sanzioni la *mancata risposta alle richieste di controllo entro 30 giorni* come **violazione dei doveri d'ufficio**, la quale viene anche presa in considerazione ai fini della misurazione e della valutazione della *performance* individuale dei responsabili dell'omissione (v. anche *infra*).

In maniera simmetrica è previsto dal T.U. in materia di trasparenza delle pubbliche amministrazioni (d.Lgs. 33/2013) che sul sito istituzionale di ogni P.A. siano pubblicati:

- i **recapiti telefonici e la casella di posta elettronica** dell'ufficio responsabile ai sensi degli artt. 43, 71 e 72 D.P.R. 445/2000;
- le **convenzioni quadro** ex art. 58 del Codice dell'amministrazione digitale;
- le ulteriori modalità per la **tempestiva acquisizione d'ufficio** dei dati e per lo svolgimento dei controlli sulle dichiarazioni sostitutive da parte delle amministrazioni procedenti.

La violazione dei doveri d'ufficio

Ai sensi dell'art. 74 D.P.R. 445/2000, costituisce **violazione dei doveri d'ufficio** la **mancata accettazione delle dichiarazioni sostitutive di certificazione o di atto di notorietà** rese in ossequio a quanto disposto dal T.U. medesimo.

Costituiscono, inoltre, violazioni dei doveri d'ufficio:

- la **richiesta e l'accettazione** di certificati o di atti di notorietà;
- il **rifiuto** da parte del dipendente addetto, di **accettare** l'attestazione di stati, qualità personali e fatti mediante l'esibizione di un documento di riconoscimento;
- il **rilascio di certificati non conformi** a quanto previsto all'articolo 40, comma 2 (secondo cui, lo ricordiamo, sulle certificazioni da produrre ai soggetti privati deve essere apposta, a pena di nullità, la dicitura: "*Il presente certificato non può essere prodotto agli organi della pubblica amministrazione o ai privati gestori di pubblici servizi*").

Assenza di responsabilità della pubblica amministrazione

L'articolo 73 d.P.R. 445/2000 dispone che le pubbliche amministrazioni ed i loro dipendenti, salvi i casi di dolo o colpa grave, sono **esenti da ogni responsabilità** per gli atti emanati, quando l'emanazione sia conseguenza di **false dichiarazioni o di documenti falsi o contenenti dati non più rispondenti a verità**, prodotti dall'interessato o da terzi.

Questa esenzione da responsabilità, tuttavia, non è assoluta. È esclusa, come anticipato:

- quando il dipendente pubblico abbia **fraudolentemente ed intenzionalmente** usato con consapevolezza le false dichiarazioni;
- nel caso in cui il dipendente **non abbia**, con la diligenza e la perizia richiesta dalla sua professionalità, **svolto con la dovuta attenzione e cura l'attività di controllo sulle dichiarazioni ed i documenti**.

Fuori da questi casi, il funzionario e l'amministrazione di appartenenza non possono essere chiamati a rispondere, ad esempio, per il danno subito da un terzo per effetto del provvedimento favorevole emanato nei confronti del richiedente che ha falsificato la dichiarazione o il documento. Né risponde in via amministrativa dell'eventuale esborso di denaro conseguente all'emanazione del provvedimento positivo. È una norma di tutela, quanto mai opportuna esistendo il principio dell'obbligo di emanare il provvedimento amministrativo prima dell'effettuazione dei controlli.

Art.71 - Modalità dei controlli da parte di Privati

Previo appositi accordi e allegando il consenso dell'interessato, il privato può chiedere alla P.A. conferma scritta dei dati autocertificati o dichiarati dall'interessato.

Comunicazioni di dati senza consenso dell'interessato, sono punibili al risarcimento dei danni da parte di chi ha effettuato la comunicazione, a norma della legge sulla Privacy.

Privacy

- La modulistica sull'autocertificazione utilizzata dalla P.A. per le proprie procedure, **deve** riportare il riferimento all'art.10 della legge n.675 sulla Privacy.
- L'art.16 prescrive che i certificati e i documenti trasmessi ad altre P.A. possono contenere **soltanto le informazioni relative a stati, fatti e qualità personali previste dalla normativa e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite**

Regime fiscale

Tutta la documentazione amministrativa è soggetta all'imposta di bollo (d.P.R. 642/1972) ed eventualmente ai diritti di segreteria (tab.D L.604/1972). Sono previste, **per legge**, **esenzioni** da questa imposta e dai diritti di segreteria in relazione all'uso cui è destinato il certificato o l'autenticazione.

Sono previste **sanzioni** in caso di mancato assolvimento dell'imposta di bollo. Le sanzioni vengono applicate a **chi rilascia l'atto, a chi lo riceve e a chi lo utilizza**.

Chi non corrisponde, in tutto o in parte, l'imposta di bollo dovuta è soggetto, oltre al pagamento del tributo, ad una sanzione amministrativa dal cento al cinquecento per cento dell'imposta o della maggiore imposta.

ATTI	BOLLO	ESENZIONI
ISTANZE	Art.3 all.A d.P.R.642/1972. Sempre imposta di bollo, salvo non sia prevista specifica esenzione	Quelle previste dalla tab.B d.P.R. 642/1972 + quelle previste da leggi speciali
AUTENTICHE DI FIRMA (se diretta a soggetto privato) E COPIA	Art.1 all.A d.P.R.642/1972. Sempre imposta di bollo, salvo non sia prevista specifica esenzione	Quelle previste dalla tab.B d.P.R. 642/1972 + quelle previste da leggi speciali
DICHIARAZIONI SOSTITUTIVE (se dirette a P.A.)	MAI	Art.37 c.1 del presente T.U.
LEGALIZZAZIONI DI FOTO	MAI	Art.34 c.2 del presente T.U. 54

Documentazione Informatica

Nei Capi II e III vengono riproposte le norme cosiddette di stile dei documenti amministrativi e tutte le norme sul documento informatico e sul suo trattamento

Non sono novità assolute (d.P.R. 513/97) però in questo contesto fanno apparire il documento informatico come la **norma** dell'attività dalla P.A. e il documento cartaceo come **l'eccezione**

Art.7 - Redazione e stesura di atti pubblici

I decreti, gli atti ricevuti dai notai, la certificazione e tutti gli atti pubblici sono redatti con qualunque mezzo idoneo atto a garantire la conservazione nel tempo.

Il testo degli atti pubblici comunque redatti non deve contenere lacune, aggiunte, abbreviazioni, correzioni, alterazioni o abrasioni.

Sono ammesse abbreviazioni, acronimi ed espressioni in lingua straniera di uso comune.

Qualora si renda necessario apportare variazioni al testo, si provvede in modo che la precedente stesura resti leggibile.

Sistemi di gestione informatica dei documenti

Gli articoli da 50 a 70 del T.U. trattano della **gestione informatica dei documenti**, cioè di quelle disposizioni che, abrogando la precedente normativa (di origine napoleonica e asburgica), introducono un nuovo sistema di:

- **protocollazione informatica di atti**
- **accesso informatico ai procedimenti**
- **archivio informatico**

dal 1° gennaio 2004 tutta la P.A deve utilizzare queste procedure

La complessità della gestione dei procedimenti digitali

L'introduzione della gestione elettronica dei flussi documentali, richiede di affrontare numerose criticità e problemi:

- **Aspetti di natura tecnica:** necessità di realizzare complesse infrastrutture con caratteristiche di alta affidabilità e sicurezza; necessità di integrazione tra diversi sottosistemi (sistemi di messaggistica, infrastrutture per la firma digitale, ...)
- **Aspetti di natura organizzativa:** necessità di avere il coinvolgimento dei livelli decisionali e politici (*commitment*); superamento di gap culturali
- **Aspetti di natura gestionale:** necessità di trattare con grandi archivi; sistemi di classificazione complessi; gli aspetti della conservazione nel tempo assicurando consistenza, integrità, accessibilità e fruibilità delle informazioni
- **Aspetti di natura culturale:** Diverso approccio tra mondo cartaceo (documento materiale) e documento informatico (documento immateriale); necessità di portare ad unitarietà la gestione dei dati con la gestione dei documenti (non strutturati)

Elementi della gestione dei documenti digitali

- 1. Documento informatico**
- 2. Firma elettronica**
- 3. Protocollo informatico**
- 4. Piano di Fascicolazione**
- 5. Canali di comunicazione**
- 6. Sistema di conservazione**

AgID, DigitPA, CNIPA

L'**Agenzia per l'Italia digitale (AgID)** è una agenzia pubblica italiana di origine governativa. L'Agenzia è sottoposta ai poteri di indirizzo e vigilanza del presidente del Consiglio dei ministri.

Svolge le funzioni ed i compiti ad essa attribuiti dalla legge al fine di perseguire il **massimo livello di innovazione tecnologica nell'organizzazione e nello sviluppo della P.A.** e al servizio dei cittadini e delle imprese, nel rispetto dei principi di legalità, imparzialità e trasparenza e secondo criteri di efficienza, economicità ed efficacia.

La struttura incorpora ed eredita le competenze precedentemente assegnate *all'Agenzia per la diffusione delle tecnologie per l'innovazione*, a *DigitPA* (già *CNIPA*) ed al *Dipartimento per l'innovazione tecnologica*.

Il documento amministrativo

Ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle PA o, comunque, utilizzati ai fini dell'attività amministrativa.

Il documento informatico

E' la "rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti".

La formazione del documento informatico è regolata dal dPCM 13.12.2014 in materia di formazione, trasmissione, conservazione copia, duplicazione, riproduzione e validazione temporale dei documenti informatici.

Le principali proprietà sono:

- **Qualità:** capacità di mantenere inalterata nel tempo forma e contenuto
- **Integrità:** possibilità di accertare che il contenuto è inalterato
- **Autenticità:** riconducibilità certa all'autore
- **Associazione ad un insieme di metadati** che permettono di conoscere il contesto, la localizzazione, il diritto all'accesso

CARATTERISTICHE CHE RENDONO PROBATORIO IL DOCUMENTO

Formazione del documento informatico

La formazione del Documento Informatico può avvenire:

1. redazione tramite l'utilizzo di appositi strumenti software
2. acquisizione per via telematica o da supporto informatico
3. acquisizione della copia per immagine su supporto informatico di un documento analogico
4. acquisizione della copia informatica di un documento analogico
5. registrazione informatica delle informazioni risultanti da transazioni o processi informatici, oppure dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente
6. generazione o raggruppamento, anche in via automatica, di un insieme di dati o registrazioni, provenienti da una o più basi dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Le caratteristiche del documento informatico

Le caratteristiche di immutabilità e di integrità sono determinate da una o più delle seguenti operazioni:

1. la sottoscrizione con **firma digitale** ovvero con firma elettronica qualificata;
2. l'apposizione di una **validazione temporale**;
3. il trasferimento a soggetti terzi con **posta elettronica certificata (PEC)** con ricevuta completa;
4. la memorizzazione su sistemi di **gestione documentale** che adottino idonee politiche di sicurezza;
5. il versamento ad un **sistema di conservazione**.

Formati di redazione utili per la conservazione

La scelta dei formati idonei alla conservazione oltre al soddisfacimento delle caratteristiche deve essere strumentale alle caratteristiche di **immodificabilità** e staticità nel tempo

- E' opportuno privilegiare i formati che siano **standard internazionali** o, quando necessario, formati proprietari le cui specifiche tecniche siano pubbliche
- Ulteriore elemento di valutazione nella scelta del formato è il **tempo di conservazione** previsto dalla normativa per le singole tipologie di documenti informatici.
- I formati per la conservazione adottati per le diverse tipologie di documenti informatici devono essere indicati nel **manuale di conservazione** motivandone le scelte effettuate

Formati attualmente normati: PDF - PDF/A - gif, .jpg, .tif - OOOXML - Office Open XML (principali estensioni: .docx, .xlsx, .pptx) - Open Document Format - TXT (codifica Unicode UTF8) – XML - Messaggi di posta elettronica (EML)

Non esiste un solo formato: è necessario sceglierlo adeguato alla rappresentazione del contenuto

La firma elettronica

Il Regolamento eIDAS disciplina tre tipologie di firme elettroniche:

1. **Firma Elettronica** - dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.
2. **Firma Elettronica Avanzata (FEA)** - firma elettronica che soddisfa i seguenti requisiti:
 - è connessa unicamente al firmatario;
 - è idonea a identificare il firmatario;
 - è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
 - è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
3. **Firma Elettronica Qualificata (FEQ)** – che in aggiunta a quelle di una firma elettronica avanzata possiede queste caratteristiche:
 - è creata su un dispositivo qualificato per la creazione di una firma elettronica
 - è basata su un certificato elettronico qualificato
 - ha effetto giuridico equivalente a quello di una firma autografa.

La firma (avanzata) digitale

Nella **sola normativa italiana** esiste inoltre 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”*

La firma digitale conferisce al documento informatico le seguenti caratteristiche:

- **autenticità**: la firma digitale garantisce l'identità del sottoscrittore del documento;
- **integrità**: la firma digitale assicura che il documento non sia stato modificato dopo la sottoscrizione;
- **non ripudio**: la firma digitale attribuisce piena validità legale al documento, pertanto il documento non può essere ripudiato dal sottoscrittore:

“il documento informatico, cui è apposta una firma elettronica, soddisfa il requisito della forma scritta e sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità” (Art. 21 CAD)

Tipologie di firma elettronica

Tipo di firma	Descrizione	Requisiti del Certificatore	Funzione dei certificati	Effetti
ELETTRONICA	Dati elettronici allegati o connessi a documenti informatici per fini di autenticazione	Requisiti di onorabilità degli amministratori ex T.U. sull'attività bancaria e creditizia. L'attività è libera e non necessaria di autorizzazione preventiva	Collegano la firma elettronica al titolare e ne confermano l'identità	Sul piano probatorio, i documenti con tale firma sono liberamente valutabili in base alle caratteristiche di qualità e sicurezza del sistema di firma utilizzato.
ELETTRONICA AVANZATA	Firma elettronica che garantisce anche l'integrità del documento e creata con mezzi sui quali il firmatario ha un controllo esclusivo			
ELETTRONICA QUALIFICATA	Firma elettronica avanzata, creata con dispositivo "sicuro", con certificato rilasciato da un Certificatore qualificato	Come sopra, più altri requisiti di affidabilità (organizzativa, tecnica, finanziaria, ...). E' richiesta una comunicazione di inizio attività al M.I.T.	Contengono i dati previsti dalla normativa, firmati digitalmente dal Certificatore che li ha rilasciati. L'emissione, revoca e sospensione sono oggetto di pubblicazione	Sul piano probatorio, i documenti con tali firme fanno piena prova di autenticità fino a querela di falso
DIGITALE	Firma elettronica qualificata con certificato rilasciato da un Certificatore accreditato	Come sopra, più forma di società di capitali e capitale sociale non inferiore a quello per l'attività bancaria. E' richiesto l'accreditamento presso il M.I.T.		

Differenze tra firma elettronica e firma digitale

	Firma elettronica	Firma digitale
Creazione mediante algoritmo	Non specificato	SI
Ripudiabilità in sede di giudizio	Non riconoscimento	Querela di falso
Copia indistinguibile dall'originale	SI	SI
Opponibilità in sede di giudizio	Forse	SI
Emessa da un certificatore accreditato	NO	SI

Efficacia giuridica della firma digitale nella normativa comunitaria: firma “leggera” e firma “forte”

La struttura normativa dettata dal legislatore comunitario ha introdotto differenti livelli di sottoscrizione che nel linguaggio corrente hanno iniziato a essere identificate come firma “**debole**” o “**leggera**” e firma “**forte**” o “**pesante**”.

Ovviamente l’efficacia giuridica delle due firme è diversa. **La firma digitale è equivalente a una sottoscrizione autografa. Le altre potrebbero non esserlo** e vengono valutate in fase di giudizio in base a caratteristiche oggettive di qualità e sicurezza.

Nell’utilizzo del documento informatico, quando si ha la necessità di una sottoscrizione **equivalente a quella autografa è indispensabile utilizzare la firma digitale**. Negli altri casi, più che di un processo di firma si tratta di un **processo di autenticazione con minori requisiti di sicurezza e quindi con una minore efficacia probatoria**.

Il valore legale della firma digitale in Italia

Art.21, c.2, CAD (già art.10 d.P.R. 445/2000): *“Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che questi dia prova contraria”*

Art. 2702 del c.c: *“La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta”.*

Quindi **la firma digitale è equiparata alla scrittura privata sottoscritta con firma autografa**, ma con una sostanziale differenza:

- la firma autografa non autenticata, può essere **disconosciuta** dal sottoscrittore, ed è la controparte a doverne dimostrare la paternità;
- l'utilizzo della firma digitale si **presume riconducibile al titolare** salvo che questi ne dia prova contraria (**come se fosse una firma autenticata**), invertendo in tal modo l'onere della prova: è il sottoscrittore che, per vederne nulli gli effetti, deve intentare un a querela di falso.

Valore legale dei documenti informatici stampati

La firma digitale è stata individuata dal CAD come la soluzione ai problemi di non modificabilità, integrità e non ripudio dei documenti elettronici.

Ma quando un documento elettronico è stampato, tutti gli attributi dati dalla firma digitale sono definitivamente persi, quindi il documento stampato necessiterebbe di essere nuovamente autenticato con i tradizionali metodi, perdendo così i vantaggi di essere nato in formato elettronico e di essere stato firmato in maniera digitale.

Per risolvere questo inconveniente il metodo che sta riscuotendo i maggiori consensi e che si sta diffondendo più rapidamente è quella dei cosiddetti **TIMBRI DIGITALI**.

Il Timbro digitale

Con i timbri digitali il documento elettronico firmato è trasformato in un codice grafico bidimensionale capace di contenere l'intero documento e la sua firma digitale.

Questo accorgimento permette di realizzare documenti cartacei che riportino stampate, e leggibili, solo le informazioni pubbliche del documento, **mantenendo tutte le informazioni riservate e/o sensibili crittografate all'interno dello stampato**. L'accesso a queste informazioni sarà consentito solo a coloro che hanno le necessarie autorizzazioni.

Ex.: Supponiamo che un cittadino richieda un documento ufficiale, ad esempio una concessione. L'amministrazione, dopo aver eseguito tutte le procedure per firmarlo in maniera digitale, rilascia il documento in formato elettronico comprensivo del timbro digitale. Il cittadino scarica il documento e stampa il documento così ottenuto completo di timbro digitale. A questo punto la verifica dell'autenticità del documento può essere effettuata a partire dal documento in formato cartaceo acquisendo il documento attraverso uno scanner. Al termine di questa operazione l'informazione contenuta nel timbro è elaborata da un software di decodifica per estrarne tutte le informazioni utili all'autenticazione del documento.

Validazione Temporale nei documenti e processi informatici

La necessità di attestare una data ed ora è richiesta per validare temporalmente le nuove comunicazioni digitali, i flussi informatici, i log generati da un Log Management System o i registri cronologici di dati.

Il legislatore prevede ai sensi dell'art. 20, c.3, del CAD che ***“la data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.”***

Le regole tecniche sulla validazione temporale sono definite nel dPCM 22/02/2013, in cui all'art.41 sono indicati i possibili riferimenti temporali opponibili a terzi, quali:

1. i riferimenti temporali realizzati dai certificatori accreditati mediante marche temporali;
2. i riferimenti temporali apposti sul giornale di controllo da un certificatore accreditato secondo la scala di tempo UTC (IEN) con una differenza non superiore ad un minuto primo;
- 3. il riferimento temporale contenuto nel protocollo informatico;**
- 4. il riferimento temporale ottenuto con la conservazione dei documenti in conformità alle norme vigenti, ad opera di un pubblico ufficiale o di una PA;**
- 5. il riferimento temporale ottenuto attraverso l'utilizzo di posta elettronica certificata (PEC);**
6. l'utilizzo della marcatura postale elettronica ai sensi dell'art. 14, comma 1, punto 1.4 della Convenzione postale universale.

La digitalizzazione dei processi amministrativi

La **digitalizzazione dei procedimenti amministrativi** consente:

- nuove modalità di comunicazione e interazione con l'utenza attraverso l'erogazione di servizi e la realizzazione di un **unico punto di accesso**
- di **controllare tutte le fasi del ciclo**, dalla sua creazione/acquisizione fino alla sua archiviazione finale, controllando tutto ciò che sta "nel mezzo": validazione, approvazioni, visti, firme, e includendo la possibilità di visualizzare lo stato degli avanzamenti, i ritardi e gli accessi
- di costruire processi di **trasparenza amministrativa**: per costruire una PA trasparente è necessario avere una adeguata informatizzazione

I procedimenti amministrativi incentrati sulla **gestione documentale** garantiscono la corretta gestione dell'intero **ciclo di vita dei documenti**, dalla produzione alla conservazione. I sistemi per la gestione documentale consentono infatti di:

- **Automatizzare** i processi di classificazione, fascicolazione e definizione dei metadati (informazioni base e specifiche per tipologia di documenti)
- **Automatizzare** la fase di registrazione dei documenti in ingresso e uscita e assegnazione alle unità organizzative
- **Dematerializzare** il trattamento dei flussi documentali in ingresso e in uscita
- **Supportare** l'archiviazione dei documenti informatici e delle copie

La gestione documentale

Sistema di Protocollo conforme alle Regole tecniche per il Protocollo informatico (DPCM 3 dicembre 2013, con caratteristiche tecniche descritte dal decreto in materia di protocollo informatico, oppure l'invio in conservazione del registro giornaliero di protocollo, ecc.).

Gestione di documenti informatici e non cartacei: **adozione di un modello organizzativo** (flussi, figure professionali, soluzione di gestione e conservazione documentale) che ne consenta la formazione e validazione conformemente alle regole tecniche del dPCM 13/11/2014 e del dPCM del 3/12/2013.

Adozione e costante aggiornamento delle **regole di gestione e archiviazione** tramite provvedimenti obbligatori quali il **manuale di gestione documentale** e il **manuale di conservazione**, loro diffusione e pubblicazione.

Adozione di un sistema di gestione a norma e sua integrazione con ogni applicazione che produce o riceva documenti informatici, per consentire **la formazione e la futura conservazione dei fascicoli** e la validità del valore probatorio dei documenti nel tempo.



La posta elettronica

L'utilizzo della posta elettronica quale valido mezzo di trasmissione di documenti informatici era già previsto dall'art. 14 del d.P.R. n. 445/2000 (ora art.45 del CAD), che consente di utilizzare la posta elettronica quale **strumento sostitutivo o integrativo di quelli già ordinariamente utilizzati.**

La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, in data 27/11/2003, ha emesso una **direttiva sull'impiego della posta elettronica nelle PA**, tutt'ora valida e attuale.

Le caselle di posta istituzionali – problemi gestionali

La direttiva, oltre a prevedere di dotare ogni dipendente pubblico di una casella di PE (“... *anche quelli per i quali non sia prevista la dotazione di un personal computer*”), dispone di attivare “... *apposite* **CASELLE ISTITUZIONALI affidate alla responsabilita' delle strutture di competenza.** Queste ultime dovranno procedere alla tempestiva lettura, **almeno una volta al giorno**, della corrispondenza ivi pervenuta, adottando gli opportuni metodi di conservazione della stessa in relazione alle varie tipologie di messaggi ed ai tempi di conservazione richiesti”

Contenuti della posta elettronica

Sempre la direttiva stabiliva che la posta elettronica “... può essere utilizzata per la **trasmissione di tutti i tipi** di informazioni, documenti e comunicazioni in formato elettronico ...”, ed in particolare:

1. **richiedere o concedere ferie o permessi**
2. **richiedere o comunicare designazioni in comitati**, commissioni, gruppi di lavoro o altri organismi
3. **convocare riunioni**, inviare comunicazioni di servizio ovvero notizie dirette al singolo dipendente
4. diffondere **circolari** o ordini di servizio
5. **trasmettere copie di documenti redatti su supporto cartaceo** con il risultato, rispetto al fax, di ridurre tempi, costi e risorse umane da impiegare, soprattutto quando il medesimo documento debba, contemporaneamente, raggiungere piu' destinatari
6. e' un efficace strumento per la trasmissione dei **documenti informatici sottoscritti** ai sensi della disciplina vigente in materia di firme elettroniche

Quanto alla certezza della ricezione del suddetto documento da parte del destinatario, il mittente, puo' richiedere al destinatario stesso un messaggio di risposta che confermi l'avvenuta ricezione.

... le amministrazioni devono dotare tutti i loro dipendenti di una casella di posta elettronica ...”

Inoltre l'art.47, c.3, lett.B del CAD, ha previsto che dal novembre 2005, le PA devono provvedere a **“utilizzare la PE per le comunicazioni tra l'amministrazione e i propri dipendenti...”**

Sicurezza e trasmissione tramite posta elettronica

Nel momento in cui trasmettiamo un documento informatico tramite la posta elettronica, dobbiamo soddisfare diverse esigenze:

- *certezza dell'integrità del messaggio*
- *data e ora di spedizione e ricezione*
- *prova dell'avvenuta ricezione*
- *prova dell'apertura e lettura del messaggio e suoi allegati*
- *privacy*
- *non ripudio, ovvero la prova da chi sono partiti i dati e a chi sono arrivati*

La prima esigenza può essere soddisfatta con l'utilizzo della firma digitale.

Le altre, per la PA, sono state soddisfatte dal legislatore tramite l'adozione di uno strumento informatico chiamato **Posta Elettronica Certificata (PEC)**

Posta Elettronica Certificata (PEC)

La PEC consiste in un sistema di posta elettronica (*si tratta di una casella di posta elettronica diversa da quella tradizionale*) nel quale, a seguito dell'invio di comunicazioni e documenti informatici, viene fornita al mittente un'**attestazione elettronica, con valenza legale, in merito all'invio e alla consegna di quanto inoltrato**. Un sistema molto simile a quello delle raccomandate postali r/r. Tuttavia, il sistema di posta elettronica certificata risolve alcune carenze intrinseche della raccomandata tradizionale:

- **la conoscibilità certa della casella mittente** e, quindi, del titolare della casella di PEC, (mentre non è tracciato con certezza colui che spedisce una raccomandata);
- la possibilità di **legare in maniera certa ed opponibile** la trasmissione con il documento trasmesso.

Confronto PEC e altri sistemi di invio di documenti

	PEC	Racc. r/r	Email	fax
Validità legale	SI	SI	NON CERTA	SI
Ricevuta di avvenuta consegna	SI	SI	NON AUTOMATICA	SI
Inalterabilità del messaggio	SI	NO	NO	SI
identità mittente/destinatario	SI	NO	NO	NO
Velocità di consegna	SI	NO	SI	SI
Semplicità e comodità d'uso	SI	NO	SI	SI
Accesso da postazioni diverse	SI		SI	SI
Eliminazione problemi di phishing (spillaggio di dati personali)	SI		NO	
Costi fissi	SI	NO	SI	NO

Invio e ricezione della PEC

"**Certificare**" l'invio e la ricezione sono i due momenti fondamentali nella trasmissione dei documenti informatici: significa fornire al mittente una ricevuta che costituisce **prova legale** dell'avvenuta spedizione del messaggio e dell'eventuale allegata documentazione.

Allo stesso modo, quando il messaggio perviene al destinatario, il gestore invia al mittente la **ricevuta di avvenuta (o mancata) consegna** con precisa indicazione temporale.

Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte è conservata per un periodo di tempo definito a cura dei gestori (minimo 30 mesi art 11, c. 2, d.P.R. 68/2005), **con lo stesso valore giuridico delle ricevute**.

È importante sottolineare che la PEC offre la garanzia della consegna del messaggio e **non della sua lettura** da parte del destinatario. In altre parole nulla è detto sul fatto che il destinatario abbia letto o meno il messaggio PEC, ma si hanno garanzie sull'avvenuto recapito. Il che, in termini legali, equivale alla raccomandata con ricevuta di ritorno, ma con in più la prova certa del contenuto.

Riassumendo

Nel circuito PEC vengono rilasciate:

<p>tre ricevute ai fini della certificazione del messaggio di posta elettronica certificata</p>	<p>Di accettazione, che attesta l'avvenuto invio della mail dal gestore di posta elettronica certificata del mittente</p>
	<p>Di presa in carico, che attesta il passaggio di responsabilità tra due distinti gestori di posta certificata, mittente e destinatario. Questa ricevuta viene scambiata tra i due gestori e non viene percepita dagli utilizzatori del servizio</p>
	<p>Di avvenuta consegna, che attesta che il messaggio è giunto a buon fine e che il destinatario ne ha piena disponibilità nella sua casella (anche se non ha ancora visto il messaggio)</p>
<p>In caso di situazione negativa esistono inoltre tre tipi di avvisi rilasciati dal sistema PEC:</p>	<p>Di non accettazione (per virus, utilizzo di un mittente falso o utilizzo di destinatari in copia nascosta, vietati dalla PEC, o altri problemi)</p>
	<p>Di mancata consegna, che sarà inviata al mittente entro 24 ore</p>
	<p>Di rilevazione di virus informatici</p>
<p>Si aggiunge che i messaggi in ingresso al sistema PEC possono essere “imbustati” dal gestore in due differenti tipologie di buste:</p>	<p>Di trasporto, se il messaggio proviene da una casella di PEC e supera tutti i controlli di esistenza, provenienza e validità della firma</p>
	<p>Di anomalia, se il messaggio proviene da una casella non PEC oppure è malformato</p>

I vantaggi della PEC

1. **Ogni formato digitale** può essere inviato tramite PEC;
2. I messaggi possono essere consultati da **ogni computer** connesso a internet;
3. Vengono certificati anche gli **allegati** al messaggio;
4. L'avvenuta consegna della mail viene **garantita**, nel caso non sia possibile consegnare il messaggio l'utente viene informato;
5. Le ricevute di consegna hanno **validità legale**;
6. **Tracciabilità** della casella mittente e conseguentemente del suo titolare;
7. **Certezza** sulla destinazione dei messaggi;
8. L'invio dei messaggi **può avere costi inferiori** a quello delle raccomandate. Il gestore rende disponibile una casella PEC con un costo calcolato su base annuale. Solitamente una volta pagato il canone annuale l'utente può inviare un numero illimitato di messaggi PEC (costo PEC Comune di Mirandola: 250,00 Euro per 3 anni)
9. Elevati requisiti di **qualità e continuità** del servizio;
10. Obbligo da parte del gestore di archiviare tutti gli eventi associati ad invii e ricezioni di messaggi PEC, per un periodo di **30 mesi**;
11. Obbligo da parte del gestore di applicare le procedure atte a garantire il **rispetto delle misure di sicurezza** previste dal CAD.
12. I servizi di posta elettronica certificata resi disponibili dai gestori iscritti nell'elenco pubblico risultano **interoperabili**. Questo significa che due utenti appartenenti a differenti gestori possono scambiare PEC con le stesse garanzie di due utenti appartenenti allo stesso gestore.

Svantaggi della PEC

1. **Non gratuita** (almeno per coloro che non usufruiranno delle offerte pubbliche), a differenza di altri sistemi;
2. Lo spazio della casella PEC **non è infinito**;
3. Il messaggio è conservato nel server del ricevente per almeno 30 mesi, ma la legge **non stabilisce cosa ne accadrà dopo tale periodo**;
4. La PEC **non è uno standard internazionale** ma solo italiano, pertanto non è interoperabile con altri sistemi (tipo S-MIME o PGP);
5. Non è un protocollo di trasmissione ma un software di gestione di casella di posta, e per gestire la PEC ci si deve dotare di un **nuovo indirizzo di posta elettronica**, al contrario di altri sistemi di certificazione;
6. Se il PC del destinatario è spento o non collegato alla rete, **non viene notificato alcun avviso** che rimarrà memorizzato sul server del gestore;
7. Il contenuto delle buste PEC è **visionabile e modificabile dal gestore di PEC**, e resta nella sua disponibilità per lunghi periodi. Inoltre l'accumularsi nei server di pochi gestori di un'enorme quantità di dati, è un sicuro richiamo per gli hacker (e per chiunque volesse effettuare delle intercettazioni ambientali);
8. Affinchè la procedura vada a buon fine è necessario che **sia il mittente che il destinatario abbiano una PEC**;
9. Possibile diffusione di **spamming certificato** e **spam phishing**, sistemi volti a frodare i destinatari grazie alla suggestione, da parte del ricevente, di ricevere messaggi da fonti attendibili
10. Un messaggio trasmesso da una PEC può giungere anche ad una casella di posta tradizionale, ma senza che ciò renda **possibile attivare tutte le procedure di conferma relative alla consegna del messaggio**. Pertanto, anche se è possibile leggere o rispondere al messaggio, **questo non avrà alcun valore giuridico**. Nel nostro caso, inoltre, ciò comporta l'impossibilità di trattare il messaggio e il suo contenuto con gli strumenti automatizzati del protocollo informatico (in questo caso l'attribuzione del numero di protocollo sarebbe possibile solo con la stampa del documento che, essendo documento informatico, non avrebbe più valore di originale). **Pertanto è necessario adottare tutte le misure affinché il mittente diriga il messaggio alla casella di PEC istituzionale.**

Categorie soggette al possesso di PEC

Soggetti	Obblighi	Cosa è possibile fare con la PEC
PA	Obbligo di dotarsi di PEC entro gennaio 2006 , e obbligo entro giugno 2009 di pubblicare l'indirizzo di PEC sulla home page del proprio sito web	Inviare documenti ogni volta che è necessario avere certezza della loro ricezione, e per ogni comunicazione con cittadini e imprese
Cittadini	Facoltativa. Possibilità di richiedere da aprile 2010 PEC (CEC-PAC) gratuita (sperimentazioni di INPS e ACI dal 2009). ORA "DOMICILIO DIGITALE": art.3bis del CAD	Con la PEC gratuita (CEC-PAC) è possibile dialogare in modo esclusivo, sicuro e non oneroso con la PA
Liberi professionisti	Obbligo di dotarsi di PEC entro novembre 2009	Gestire comunicazioni ufficiali con tutta la PA e gli enti previdenziali; inviare e ricevere contratti e fatture; sostituire le raccomandate a/r
Società o imprese individuali già iscritte	Obbligo di dotarsi di PEC entro novembre 2009 (30/06/13 per le imprese individuali)	Gestire tutte le comunicazioni con INPS e INAIL, Camere di commercio, Agenzia delle entrate, e con la PA in generale; inviare ordini, contratti e fatture
Nuove società e imprese individuali	Al momento dell'iscrizione alla Camera di commercio devono dichiarare il possesso della PEC. In caso contrario è la CdC ad attribuire d'ufficio una PEC	

PEC e PA

Secondo l'art.16bis, c.6, del decreto anticrisi, ogni PA deve utilizzare **unicamente la PEC**, con effetto equivalente alla notificazione per mezzo della posta, **per le comunicazioni e le notificazioni aventi come destinatari dipendenti della stessa o di altra PA.**

Inoltre secondo quanto stabilito dal c.8, le PA devono istituire una casella di PEC per ciascun registro di protocollo e ne danno comunicazione al CNIPA (ora Agid) che provvede alla pubblicazione di tali caselle in un **elenco consultabile per via telematica**, e secondo quanto stabilito dalla lettera *b*) del comma 1 dell'art.34 della L. 69/2009, dal 30.06.09 deve essere pubblicato nella pagina iniziale del sito web di ogni PA un indirizzo di PEC a cui il cittadino possa rivolgersi per qualsiasi richiesta.

Sempre relativamente agli obblighi delle PA, il CAD all'art.54, c.1, lett.d, precisa che i siti della PA devono contenere **l'elenco completo delle casella di posta elettronica istituzionali attive**, specificando anche se si tratta di PEC, ed entro gennaio 2006 doveva essere istituita almeno 1 casella di posta elettronica istituzionale ed 1 di PEC per ciascun registro di protocollo, e ad utilizzare la posta elettronica per le comunicazioni tra le amministrazioni e i propri dipendenti.

Il domicilio digitale per i cittadini

Dopo il fallimento della CEC-PAC, è stato introdotto con il d.Lgs. N.179/2012 il **domicilio digitale**

L'articolo 3-bis del CAD sancisce che *"Al fine di facilitare la comunicazione tra PA e cittadini, è facoltà di ogni cittadino indicare alla PA [...] un proprio indirizzo di posta elettronica certificata quale suo domicilio digitale."*

Il domicilio digitale deve essere inserito nell'Anagrafe Nazionale della Popolazione Residente (ANPR) e reso disponibile a tutte le PA e ai gestori o esercenti di pubblici servizi. Il comma 4 prevede infatti che: *"a decorrere dal 1° gennaio 2013, [...] le amministrazioni pubbliche e i gestori o esercenti di pubblici servizi comunicano con il cittadino esclusivamente tramite il domicilio digitale dallo stesso dichiarato"*.

In attesa della registrazione del domicilio digitale nell'ANPR, per le sole istanze rivolte al SUAP (Sportello Unico Attività Produttive), dove è prevista la presenza di un professionista e per favorire al massimo la gestione telematica, il portale richiede di dichiarare un indirizzo PEC come domicilio digitale. Chi non possedesse un proprio indirizzo PEC può scegliere se procurarsene uno oppure può decidere di domiciliarsi presso il professionista incaricato. Questa facoltà riguarda i soli privati cittadini in quanto sia le imprese che i liberi professionisti devono già avere un indirizzo PEC.

Una volta inviata l'istanza, la PA competente comunicherà esclusivamente tramite il domicilio digitale indicato.

La conservazione del documento digitale

La conservazione del documento digitale è il nodo cruciale dell'automazione in campo documentario perché richiede un cambiamento significativo rispetto alle attività tradizionali:

- la conservazione in ambiente digitale è una **funzione attiva e continua nel tempo** per la quale non c'è ancora sufficiente esperienza, né un'adeguata analisi concettuale.
- i **tempi degli interventi** per il mantenimento della memoria si sono accorciati.
- la **diversificazione dei prodotti** non consente soluzioni univoche.
- la **fragilità dei supporti** e la **facilità nella manipolazione** richiedono investimenti significativi in termini di controllo dei depositi e sicurezza

La conservazione dei documenti - definizione

Conservare un patrimonio informativo digitale significa:

1. Mantenere nel tempo la **capacità di riprodurlo** con il contenuto e la forma originaria
2. **Proteggere** nel tempo gli archivi digitali prodotti dalle PA, impedendone il danneggiamento, la perdita o la distruzione
3. Garantire **autenticità, integrità, leggibilità e reperibilità** dei documenti nel tempo
4. Predisporre idonee misure per la qualità e la **sicurezza fisica, logica e tecnologica** dei sistemi
5. **Consentire l'accesso controllato** a dati, documenti e informazioni e la diffusione degli stessi per fini amministrativi e di ricerca; tutelare e valorizzare la memoria storica

La conservazione dei documenti – Modelli organizzativi

Modelli organizzativi:

- **in house:** La conservazione è svolta all'interno della struttura organizzativa (infrastrutture, ruoli, organizzazione appartengono all'ente)
- **In outsourcing:** La conservazione è affidata, in modo totale o parziale, esclusivamente a conservatori accreditati inseriti nell'elenco di AgID

Interrogativi

- Cosa è necessario conservare?
- Quando è necessario conservarlo?

Scadenze

- A partire dall'11 ottobre 2015 le PA sono tenute ad inviare in conservazione il registro giornaliero di protocollo entro la giornata lavorativa successiva
- Entro 31 dicembre 2016 conservazione delle fatture elettroniche 2015
- Entro 11 aprile 2017 chi effettuava "Conservazione Sostitutiva" è tenuto ad adeguarsi all'architettura OAIS

ParER

Il **Polo archivistico dell'Emilia-Romagna (ParER)**, è un servizio dell'Istituto per i Beni Artistici Culturali e Naturale dell'E.R. (IBACN), che si occupa della conservazione a lungo termine dei documenti e degli archivi digitali delle PA.

ParER è stato istituito nel 2009, **a seguito della L. regionale n.17/2008**, che affida la funzione di conservazione digitale dei documenti informatici prodotti dalla Regione e dalle altre PA dell'Emilia-Romagna all'IBACN Emilia-Romagna.

È operativo dal 2010 e alla fine del 2014 è stato **ufficialmente riconosciuto** come conservatore accreditato dall'Agenzia per l'Italia Digitale. Al momento, si tratta dell'unica struttura pubblica di questo genere operante in Italia ad essere stata accreditata.

Le attività. ParER svolge a favore degli enti le seguenti attività:

- conservazione, archiviazione e gestione dei documenti informatici
- accesso via web ai contenuti digitali in conservazione
- supporto, formazione e consulenza sulle tematiche della conservazione digitale.

Il valore aggiunto. Conservare i documenti digitali è un'attività complessa e onerosa: richiede infrastrutture e professionalità adeguate, e non tutte le amministrazioni potrebbero disporre delle risorse necessarie per svolgerla. ParER opera per sopperire a questi problemi, garantendo:

- economie di scala
- il presidio professionale, tecnologico e organizzativo sulla conservazione digitale
- la dematerializzazione dei processi e la conseguente semplificazione amministrativa
- una maggiore trasparenza e valorizzazione del patrimonio digitale delle amministrazioni
- essendo una struttura pubblica, la certezza che le attività di conservazione digitale saranno garantite in maniera costante e illimitata nel tempo.

Gli utenti di ParER. Ad oggi ParER supporta oltre 1.000 strutture pubbliche. Tra queste:

- la Regione e le sue strutture e agenzie
- le Aziende sanitarie del territorio regionale
- Province, Comuni e Unioni di Comuni, anche di altre regioni
- Università.

Sistema Pubblico di Identità Digitale (SPID)

SPID è il sistema di autenticazione che permette a cittadini ed imprese di **accedere ai servizi online della PA e dei privati aderenti con un'identità digitale unica.**

L'identità SPID è costituita da credenziali (nome utente e password) che vengono rilasciate all'utente e che permettono l'accesso a tutti i servizi online.

I tre livelli di sicurezza. Esistono tre livelli di sicurezza, ognuno dei quali corrisponde a un diverso livello di identità SPID:

- Livello 1: permette l'accesso ai servizi con nome utente e password;
- Livello 2: permette l'accesso ai servizi con nome utente e password insieme ad un codice temporaneo che ti viene inviato via sms o con app mobile dedicata;
- Livello 3: permette l'accesso ai servizi con nome utente e password e l'utilizzo di un dispositivo di accesso.

PA e privati definiscono autonomamente il livello di sicurezza necessario per poter accedere ai propri servizi digitali.

Come si ottiene l'Identità Digitale?

L'identità SPID è rilasciata dai Gestori di Identità Digitale (Identity Provider), soggetti privati accreditati da AgID che, nel rispetto delle regole emesse dall'Agenzia, forniscono le identità digitali e gestiscono l'autenticazione degli utenti.

Per ottenere un'identità SPID l'utente deve farne richiesta al gestore che preferisce e che più si adatta alle sue esigenze. Il gestore, dopo aver verificato i dati del richiedente, emette l'identità digitale rilasciando le credenziali all'utente.

Ogni gestore può scegliere tra diverse modalità di riconoscimento per verificare l'identità del cittadino.

Anagrafe Nazionale della Popolazione Residente (ANPR)

L'Anagrafe Nazionale della Popolazione Residente (ANPR) prenderà il posto delle anagrafi di tutti i Comuni italiani.

Con l'ANPR si realizza **un'unica banca dati con le informazioni anagrafiche della popolazione residente** a cui faranno riferimento non solo i Comuni, ma l'intera PA e tutti coloro che sono interessati ai dati anagrafici, in particolare i gestori di pubblici servizi.

Allineando i dati toponomastici, permetterà di concretizzare l'Anagrafe nazionale dei numeri civici e delle strade urbane (ANNCSU), strumento necessario a completare la riforma del Catasto.

Con le modifiche apportate all'art.62 del CAD si prevede che ANPR contenga, oltre ai dati anagrafici, l'archivio nazionale informatizzato dei registri di Stato civile e i dati delle liste di leva. Inoltre ANPR assicurerà ai Comuni un sistema di controllo, gestione e interscambio, puntuale e massivo, di dati, servizi e transazioni necessario ai sistemi locali per lo svolgimento delle funzioni istituzionali di competenza comunale.

Inoltre il collegamento di ANPR con l'Anagrafe Nazionale degli Assistiti (ANA) rende possibile il miglioramento dei servizi sanitari, conseguente alla maggiore efficienza del sistema sanitario e al contenimento della spesa.

ANPR conterrà anche il **domicilio digitale**.

Carta d'Identità Elettronica (CIE)

La Carta di identità elettronica è il documento personale che attesta l'identità del cittadino, realizzata in materiale plastico, dalle dimensioni di una carta di credito e dotata di sofisticati elementi di sicurezza e di un microchip a radiofrequenza (RF) che memorizza i dati del titolare.

A cosa serve

Oltre all'impiego ai fini dell'identificazione, la nuova Carta di identità elettronica può essere utilizzata per **richiedere una identità digitale sul sistema SPID**. Tale identità, utilizzata assieme alla CIE, garantisce l'accesso ai servizi erogati dalla PA.

Come si ottiene

La nuova Carta di identità elettronica si può richiedere alla scadenza della propria Carta d'identità (o in seguito a smarrimento, furto o deterioramento) presso il Comune di residenza o di dimora.

La Carta è spedita direttamente al cittadino che la riceverà entro 6 giorni dalla richiesta, presso il Comune o presso un indirizzo da lui indicato.

Il costo della Carta è di Euro 22,22, e comprende anche le spese di spedizione.

Il Progetto della CIE garantisce l'incremento dei livelli di sicurezza dell'intero sistema di emissione sia attraverso la centralizzazione della personalizzazione del supporto, sia attraverso un adeguamento delle caratteristiche del medesimo ai più avanzati standard internazionali di sicurezza in materia di documenti elettronici.

PagoPA

PagoPA è un ecosistema di regole, standard e strumenti definiti dall'AgID e accettati dalla PA, dalle Banche, Poste ed altri istituti di pagamento (Prestatori di servizi di pagamento - PSP) aderenti all'iniziativa.

PagoPA garantisce a privati e aziende:

- **sicurezza e affidabilità** nei pagamenti;
- **semplicità e flessibilità** nella scelta delle modalità di pagamento;
- **trasparenza** nei costi di commissione.

PagoPA garantisce alle PA:

- **certezza e automazione** nella riscossione degli incassi;
- **riduzione dei costi e standardizzazione** dei processi interni;
- **semplificazione e digitalizzazione** dei servizi.

PagoPA: per quali servizi può essere utilizzato

Il servizio di pagamento elettronico viene utilizzato dalle PA, dai privati e dalle aziende per riscuotere somme più o meno ingenti da parte dei propri affiliati.

I **vantaggi assicurati** agli enti beneficiari dei pagamenti sono: maggior margine di sicurezza ed affidabilità nei versamenti; flessibilità nella scelta della modalità di pagamento; maggiore semplicità dei processi di gestione; trasparenza nei costi di commissione. Le PA in particolare possono godere di una riduzione delle spese dei processi interni, grazie alla standardizzazione ed alla digitalizzazione dei servizi.

PagoPA: le modalità di pagamento

Per effettuare dei pagamenti è sufficiente selezionare uno dei tanti prestatori del servizio di pagamento, che può essere rappresentato da una banca, da un istituto di credito o da un sistema di moneta elettronica e procedere con il versamento, scegliendo uno dei canali tecnologici a disposizione. Tali canali, a loro volta, possono essere rappresentati da un conto web, un ATM o un dispositivo mobile.

Tra i vantaggi di cui l'utente può godere attraverso questo innovativo sistema di pagamento va inclusa la possibilità di conoscere preventivamente il costo dell'operazione da effettuare, ricevendo nello stesso tempo un'ulteriore garanzia dell'importo da versare. Una volta concluse le operazioni di pagamento, il contribuente riceve inoltre una ricevuta che ha valore liberatorio, ovvero può essere utilizzata come attestazione dell'avvenuto versamento.

La PA ha l'obbligo dal 2016 di far transitare i propri pagamenti sulla piattaforma PagoPA 99

PayER

PayER è la piattaforma dei pagamenti della regione Emilia Romagna che permette di effettuare transazioni online. PayER è uno Sportello Unico dei Pagamenti, attraverso il quale è possibile pagare imposte, oneri o sanzioni: dai servizi scolastici ai tributi comunali, dalle contravvenzioni agli oneri amministrativi.

Collegandosi al portale PayER si può effettuare pagamenti in favore di Comuni e Enti del territorio emiliano. Registrandosi al servizio, l'utente accede alla propria "Posizione debitoria" da dove può verificare tutte le sue pendenze nei confronti degli Enti che utilizzano la piattaforma PayER.

il servizio Payer consente di **“traghetare” facilmente su PagoPA** i servizi già configurati e attivi delle PA dell'E.R.: infatti, per tutti gli Enti soci Lepida (lo strumento operativo della Regione per l'attuazione dell'Agenda digitale), grazie agli accordi con AgID, svolge automaticamente il ruolo di “intermediario tecnologico” verso PagoPA, purché l'Ente abbia in produzione almeno un servizio configurato e attivo su PayER

La fattura elettronica

La fattura elettronica costituisce l'anello di congiunzione tra il **ciclo logistico** (contratto, ordine, consegna, fattura) ed il **ciclo finanziario** (fattura, registrazione, pagamento e riconciliazione)

Definizioni:

FATTURA: la fattura, in diritto, è un documento fiscale obbligatorio emesso da un soggetto fiscale per comprovare l'avvenuta cessione di beni o prestazione di servizi ed il diritto a riscuoterne il prezzo. E' il documento rappresentativo di un'operazione commerciale

FATTURA ELETTRONICA: la fattura elettronica indica, in Italia, una fattura in formato digitale provvista del riferimento temporale e della firma digitale dell'emittente.

La fattura, ai sensi dell'articolo 21 del D.P.R. 633/72, contiene le seguenti indicazioni:

1. Data di emissione;
2. Numero progressivo che la identifichi in modo univoco
3. Ditta, denominazione o ragione sociale, nome e cognome, residenza o domicilio del soggetto cedente o prestatore
4. Numero di partita iva del soggetto cedente o prestatore
5. Numero di partita del soggetto cessionario o committente
6. Natura, qualità e quantità dei beni e dei servizi formati oggetto dell'operazione

La fattura elettronica contiene i dati fiscalmente rilevanti ed inoltre...

1. informazioni utili per la completa dematerializzazione del ciclo passivo attraverso l'integrazione con i sistemi gestionali e/o con i sistemi di pagamento;
2. informazioni di interesse per esigenze informative concordate tra Operatori Economici o informazioni di integrità, autenticità, non ripudiabilità

L'avvio della fatturazione elettronica obbligatoria verso la PA e la conseguente costruzione dell'infrastruttura a supporto hanno permesso di creare uno standard per il mercato italiano:

- Un unico soggetto di interscambio (SDI) interfacciato con la RGS
- Un unico formato di fattura *FatturaPA* utilizzato per la formazione e trasmissione delle fatture elettroniche sia verso le PA che verso i privati

Alcuni vantaggi collegati alla Fatturazione Elettronica

Per le imprese

1. **Ottenimento dei pagamenti con tempi più rapidi**
2. **Certificazione della data di consegna e della data di ricevimento della fattura** (certificazione del credito)
3. **Maggiore competitività** (efficienza ed efficacia dei processi e nuove modalità di consegna e interscambio)
4. Contributo rilevante alla **green economy**
5. **Riduzione dei costi e tempi di trattamento della carta**
6. Accesso a **nuovi servizi finanziari**
7. **Riduzione degli errori umani tipici**
8. **Integrità sicurezza trasparenza e valore legale**
9. **sgravi fiscali** per chi aderisce alla FE B2B

Per al P.A.

1. **Rispetto delle disposizioni contro i ritardi di pagamento** nelle transazioni commerciali (D.Lgs.n.192/2012)
2. **Monitoraggio della spesa pubblica**
3. **Maggiore competitività** (efficienza ed efficacia dei processi e nuove modalità di consegna e interscambio)
4. Contributo rilevante alla **green economy**
5. **Riduzione dei costi e tempi di trattamento della carta**
6. Attivazione di **politiche premianti o sanzionatorie** verso le PA
7. **Riduzione degli errori umani tipici**
8. **Integrità sicurezza trasparenza e valore legale**