Via Satrico 14, 04100 Latina
Tel. 0773/402022 – fax 0773/1761689
ev@studiolegalevitelli.it
avvemilianovitelli@puntopec.it
www.studiolegalevitelli.it

L'Articolo 97 Costituzione:
"I pubblici uffici sono organizzati secondo disposizioni di legge, in modo che siano assicurati il buon andamento e l'imparzialità dell'amministrazione. "
Questo articolo è il punto di partenza, ma anche sempre il punto di controllo dell'intera riforma della PA.
L'intero progetto di riforma nel fondarsi sul principio di buon andamento si specifica nell'attuazione di principi di **Efficienza, Efficacia ed Economicità**
Sono concetti che qualificano i processi aziendali, in quando da una amministrazione burocratica si è inteso passare ad una amministrazione "azienda" che produce servizi.
Di qui l'obbligo per tutte le Pubbliche Amministrazioni di rendere visibile e controllabile dall'esterno il proprio operato. La trasparenza e l'obbligo di motivazione del procedimento amministrativo contribuiscono a rendere conoscibile l'azione amministrativa.

Allo stesso tempo semplificare l'attività amministrativa significa una pubblica amministrazione che costi meno alla collettività, sia in termini di stanziamenti di bilancio che in termini di costi complessivi e soprattutto che lavori meglio

Le tecnologie dell'informazione e della comunicazione fin dall'emanazione del CAD sono al centro della riorganizzazione amministrativa, quale strumento non più aggiuntivo ma ordinario e coessenziale al perseguimento degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza e semplificazione.
Tali diritti si esplicano con particolare riferimento alla **partecipazione democratica** al procedimento amministrativo (comunicazioni relative all'avvio del procedimento e alle varie fasi di esso) e al diritto di accesso ai documenti amministrativi, nel rispetto dei diritti sanciti dalla legge 7 agosto 1990, n. 241.
Va anche considerato e sottolineato che **l'erogazione dei servizi on line deve essere intesa come un'obbligazione di risultato**, che potrà considerarsi adempiuta ove le singole Pubbliche Amministrazioni garantiscano l'effettività dei singoli diritti che l'ordinamento assegna a cittadini e imprese.
Tuttavia occorre subito rammentare che un freno alla concreta attuazione del CAD è stato determinato dalla mancanza di obblighi vincolanti con relativa sanzione per le amministrazioni inadempienti. Sotto questo profilo gli adempimenti del Cad sono stati collegati alla responsabilità dirigenziale e di performance (secondo le norme del Decreto legislativo n.150/2009).

L'art. 17 del Codice dell'Amministrazione Digitale prevede che Amministrazioni centrali debbano individuare **un unico ufficio dirigenziale generale**, responsabile del coordinamento funzionale e titolare di una serie di funzioni nel campo dell'ICT, mentre l'art. 2, comma 5, dispone che il CAD si applica nel rispetto della disciplina in materia di trattamento dei dati personali.

(Art. 3) **I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni**.

Il Decreto Legislativo n. 33 del 14 marzo 2013 disciplina gli obblighi di pubblicità, trasparenza e diffusione delle informazioni sul web da parte delle Pubbliche Amministrazioni, ciò anche in attuazione della cosiddetta legge "anticorruzione" (L. n. 190/2012).
Il 19 maggio 2016 il Decreto trasparenza è stato profondamente modificato accogliendo i principi del Freedom of Information Act. Sostanzialmente si inverte la prospettiva in materia di accesso agli atti delle pubbliche amministrazioni: il cittadino ha accesso totale agli atti salve alcune limitazioni e salvo il rispetto della normativa sul trattamento dei dati personali

Allo scopo di **favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali** e **sull'utilizzo delle risorse pubbliche** e di promuovere la partecipazione al dibattito pubblico, **chiunque** ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti
L'Autorità Garante per la protezione dei dati personali con il provvedimento n. 49 del 7 febbraio 2013, ha opportunamente posto alcuni limiti al principio dell'accessibilità totale (Trasparenza Linee guida del Garante).

Le linee guida rimangono senz'altro valide ma dovranno essere sicuramente aggiornate in relazione alle modifiche apportate al decreto trasparenza

Open data

Open Data sta a significare dati pubblici in formato aperto, "libero" e accessibili a tutti i cittadini, oltre che facilmente riutilizzabili e scambiabili sul web, senza limitazioni di copyright, brevetti o altro; bidirezionalità, condivisione e partecipazione ai processi decisionali dell'amministrazione sono gli elementi che caratterizzano l'Open data e la partecipazione democratica
L'articolo 58 del CAD L'articolo 60 del CAD L'art. 52 del CAD stabilisce che i dati pubblicati senza l'espressa adozione di una licenza per il loro utilizzo si intendono rilasciati come dati di tipo aperto (open data by default).

Linee Guida Agid. I limiti alla conoscibilità dei dati rimangono sia quelli previsti dalle leggi e dai regolamenti vigenti (ad esempio in materia di segreto di Stato) sia con riferimento alla riservatezza dei soggetti a cui i dati si riferiscono (che andrà garantita ai sensi del D. Lgs. n. 196/2003).
Sono state emesse anche delle Linee Guida Valorizzazione del Patrimonio Informativo Pubblico, che tra l'altro suggerisce la necessità di costituire per avviare e gestire a regime il processo di gestione dei dati un Team Open Data inteso come il gruppo che promuove l'uso e la diffusione degli Open Data.
L'Italia ha emesso uno standard per le licenze di rilascio e utilizzabilità dei documenti posti in Open Data: Italian Open Data License.
Si ricorda tra l'altro che la PA che non pubblica gli open data ex art. 1, comma 32 (appalti) della legge n. 190 del 2012 è sanzionabile da ANAC ex art. 6, comma 11 del decreto legislativo n. 163 del 2006
In questa materia occorre anche tenere presenti le Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul Web (Deliberazione n. 88/2011 in G.U. n. 64/2011).

Siti web

Le Linee Guida indicano una lunga check list di contenuti minimi.
Gli attori della creazione, gestione e manutenzione dei siti web della PA sono: il Responsabile del procedimento di pubblicazione dei contenuti sul sito, il Responsabile dell'accessibilità informatica, il Responsabile dei sistemi informativi, Capo Ufficio stampa, Responsabile Ufficio relazioni con il pubblico.
Di fondamentale importanza nell'ambito della realizzazione del sito web distinguere i due tipi di contenuti:
- il primo sarà indirizzato dall'etichetta "Note" o "Note legali";
- il secondo dall'etichetta "Privacy" o "Protezione dei dati personali".

(Art. 53, comma 1) I siti istituzionali devono rispettare "**i principi di accessibilità, nonché di elevata usabilità e reperibilità, anche da parte delle persone disabili, completezza dell'informazione, chiarezza di linguaggio, affidabilità, semplicità di consultazione, qualità, omogeneità ed interoperabilità**". L'art. 2, Legge n. 4/2004 definisce il concetto di accessibilità come "la capacità dei sistemi informatici, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa della loro

disabilità necessitano di tecnologie assistive o configurazioni particolari". Il Web Accessibility Expert è la figura di riferimento per questa materia. Con il D.M 20 marzo 2013 i requisiti della Legge Stanca sono stati accorpati, passando da 22 a 12. E' particolarmente rilevante anche pubblicare la Dichiarazione di Accessibilità.
L'art. 4, comma 2, Legge n. 4/2004 dispone che siano nulli i contratti stipulati dalle Amministrazioni per "la realizzazione e la modifica di siti Internet quando non è previsto che essi rispettino i requisiti di accessibilità stabiliti"

(Linee Guida) Costruire un sito ben fatto significa anche seguire i principi di Costumer satisfaction ed aderire a programmi come, Mettiamoci la faccia.
Ultimamente è partito anche il progetto http://design.italia.it/, lascia tuttavia molto perplessi la totale assenza di espliciti riferimenti alla sicurezza informatica (Criticità di sicurezza per la costruzione dei siti web OSWAP 2013)

PA e Social media

L'utilizzo di social media è divenuto sempre più rilevante, tanto da imporre la pubblicazione di un vademecum, ma bisogna anche tenere conto della legge n.150/2000 (Direttiva sulla comunicazione pubblica.
Bisogna conoscere e saper utilizzare gli strumenti della comunicazione: Campagna stampa, Campagna di comunicazione e informazione, Comunicato stampa, Intervista, Manuale di immagine coordinata, Semplificazione del linguaggio, Piano di comunicazione. È fondamentale definire tanto le regole di comportamento dei dipendenti (*policy* interna), quanto quelle degli utenti e dei cittadini (*policy* esterna).
E' opportuno anche tenere in debito conto le linee guida del Garante Privacy sull'utilizzo dei social network.

Domicilio digitale del cittadino

Al fine di facilitare la comunicazione tra pubbliche amministrazioni e cittadini, è facoltà di ogni cittadino indicare alla pubblica amministrazione un proprio indirizzo di posta elettronica certificata quale suo domicilio digitale. **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.
(Art.62) E' istituita presso il Ministero dell'interno l'Anagrafe nazionale della popolazione residente (ANPR), quale base di dati di interesse nazionale. Per permettere la realizzazione dell'ANPR sono stati emanati: il DPCM del 23 agosto 2013, n.109 con le modalità di funzionamento dell'ANPR; il DPCM 10 novembre 2014, n. 194 .
In assenza del domicilio digitale le amministrazioni creeranno documenti informatici sottoscritti con firma digitale ed invieranno ai cittadini stessi, per posta ordinaria o raccomandata con avviso di ricevimento, copia analogica di tali documenti sottoscritti con firma autografa.

PEC

L'art 1, comma 1, lett. v-bis) definisce 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**; L'art. 47 pone un vero e proprio obbligo di utilizzo degli strumenti telematici nelle comunicazioni tra le Pubbliche Amministrazioni.
In tema di ricezione del messaggio, il legislatore stabilisce una vera e propria presunzione di conoscenza.
Le Pubbliche Amministrazioni comunicano o a mezzo di posta elettronica certificata oppure Attraverso l'interscambio automatico di informazioni con altri sistemi - la "cooperazione applicativa".

Rivolgendosi al gestore entro trenta mesi (o entro il periodo più lungo eventualmente previsto dai singoli contratti) il titolare della casella PEC può richiedere copia dei log. Probelma del back up delle pec
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.
In materia di comunicazioni telematiche va sempre tenuto come riferimento l'art. 49 "**Segretezza della corrispondenza trasmessa per via telematica**"; ma anche la deliberazione n. 13 del 1° marzo 2007 dell'Autorità Garante per la Protezione dei dati personali che ha inteso prescrivere ai datori di lavoro alcune misure per conformare il trattamento di dati personali, effettuato per verificare il corretto utilizzo, all'interno del rapporto di lavoro, della posta elettronica e della rete internet alle disposizioni vigenti. Nel 2015 è stato anche pubblicato il vademecum 2015 del Garante "Privacy e lavoro".

SPID

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.
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.
Deve tenersi però a mente che una volta che il sistema europeo (eIDAS) delle identità digitali sarà completo, si potranno individuare Stati che rilasciano identità digitali con maggiore facilità ed altri più esigenti
Il Sistema SPID si conforma al principio di necessità in base al quale i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi.
I trattamenti dei dati personali sono effettuati esclusivamente per le finalità previste dall'articolo 64 del CAD, nel rispetto delle garanzie previste dal medesimo decreto legislativo n. 196 del 2003.
Il rilascio delle identità digitali si articola nei seguenti processi:
a) richiesta dell'identità digitale e identificazione del richiedente;
b) esame e verifica dell'identità del richiedente;
c) conservazione e registrazione dei documenti;
d) emissione dell'identità digitale;
e) creazione e consegna delle credenziali.

CLOUD

Investire nei sistemi cloud significa implementare strumenti utili volti a privilegiando un approccio che oltre a proporsi con finalità di razionalizzazione e di risparmio miri anche a promuovere un'organizzazione innovativa dei servizi pubblici online che le soluzioni tecnologiche e operative del cloud rendono possibile.
Cloud Infrastructure as a Service - IaaS (infrastruttura cloud resa disponibile come servizio)
Il fornitore del servizio cloud offre, secondo un modello "a consumo", gli strumenti hardware e software di base
Cloud Software as a Service - SaaS (software erogato come servizio del cloud)
Il fornitore eroga via Internet una serie di servizi applicativi ponendoli a disposizione degli utenti finali.
Cloud Platform as a Service - PaaS (piattaforme software fornite via Internet come servizio)
La pubblica amministrazione che voglia acquisire prodotti e servizi cloud, pertanto, dovrà seguire le regole procedimentali necessarie per l'individuazione dell'operatore economico contraente e dovrà sottoscrivere con tale soggetto un contratto pubblico ai sensi del D. Lgs. n. 163/2006 e del relativo regolamento di esecuzione approvato con D.P.R. 207/2010

Posto che la PA che acquista servizi di cloud va senz'altro considerata titolare di trattamento, il problema si pone dal lato del cloud provider che potrebbe, a seconda dei casi, essere considerato quale titolare autonomo di trattamento o quale responsabile.

Partecipazione al procedimento amministrativo
Il procedimento amministrativo è una serie di atti ed operazioni funzionalmente collegati e coordinati, preordinati al perseguimento di uno specifico obiettivo finale
l'emissione di un provvedimento amministrativo volto alla cura di un interesse pubblico concreto ed attuale produttivo di effetti giuridici verso i destinatari.
La tutela giurisdizionale dei diritti legati al dialogo con le Amministrazioni e alla partecipazione ai procedimenti con l'ausilio delle nuove tecnologie trova ora un ulteriore strumento di tutela rappresentato dal ricorso collettivo per l'efficienza delle amministrazioni e dei concessionari di servizi pubblici (la c.d. **class action pubblica** di cui al D. Lgs. n. 198/2009).
Le PPAA devono organizzare autonomamente la propria attività, utilizzano le tecnologie dell'informazione e della comunicazione al fine di realizzare efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione, nonché garanzia dei diritti digitali dei cittadini e delle imprese.
Le pubbliche amministrazioni utilizzano le tecnologie dell'informazione e della comunicazione, garantendo 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
Le Pubbliche Amministrazioni formano gli originali dei propri documenti con mezzi informatici (art. 40 CAD Formazione documenti informatici);
Ai fini dell'avvio del procedimento amministrativo e del su0 iter le comunicazioni sono valide solo se ne sia verificata la provenienza. Ai fini della verifica della provenienza, gli strumenti necessari sono la firma digitale o elettronica qualificata, la segnatura di protocollo, la PEC oppure qualsiasi altro strumento che renda possibile accertare altrimenti la provenienza

Il fascicolo informatico

Il fulcro della nuova modalità di gestione dei procedimenti amministrativi è rappresentato dal fascicolo informatico del procedimento:
Ciascuna Pubblica Amministrazione titolare deve raccogliere in un fascicolo informatico gli atti, i documenti e i dati relativi ad ogni specifico procedimento, da chiunque formati.
Il fascicolo conserva i documenti (registrati e non registrati), classificati in maniera omogenea, relativi ad un determinato affare o procedimento amministrativo di competenza di un ufficio di una Pubblica amministrazione.
Ciascun fascicolo contiene soltanto documenti identificati con la medesima classificazione.
Gli elementi del fascicolo informatico sono indicati all'art. 41
I documenti trasmessi 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.
Le istanze e dichiarazioni da presentare per via telematica (Art. 65, comma 1 CAD) sono valide solo se:
a) vengono sottoscritte con firma digitale o firma elettronica qualificata;
b) l'autore è identificato dal sistema informatico con l'uso della carta d'identità elettronica o della carta nazionale dei servizi;
c) l'autore è identificato dal sistema informatico con SPID;
d) trasmesse dall'autore mediante la propria casella di posta elettronica certificata purché le relative credenziali di accesso siano state rilasciate previa identificazione del titolare e ciò sia attestato dal gestore del sistema nel messaggio o in un suo allegato.
e) l'art. 4 del CAD ha fissato il principio secondo cui 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 le modalità indicate dal DPR 28 dicembre 2000, n. 445, in particolare l'articolo 59 (Accesso esterno) e l'aticolo 60 (Accesso effettuato dalle pubbliche amministrazioni). Le pubbliche amministrazioni mediante proprie applicazioni informatiche accedono al sistema di gestione informatica dei documenti delle aree organizzative omogenee

Comunicazioni tra imprese e amministrazioni pubbliche

Questa norma individua nelle tecnologie dell'informazione e della comunicazione l'unico canale legittimo per lo svolgimento dei rapporti tra le Amministrazioni pubbliche e le imprese, escludendo la possibilità del ricorso a strumenti diversi, a prescindere dal soggetto (pubblico o privato) che invia la comunicazione.

Il DPCM 22/7/2011 è intervenuto in questa materia: l'art. 10 relativo allo Sportello unico per le attività produttive (SUAP); l'art. 11 sull'istituzione del Registro informatico degli adempimenti amministrativi per le imprese.

Attualmente si f riferimento anche al sito: https://www.impresainungiorno.gov.it/sportelli-suap/

Il Sistema Pubblico di Connettività (artt. 72 e segg CAD)

L'insieme di regole, standard, strutture organizzative e infrastrutture finalizzate a:

- agevolare il colloquio tra Pubblica Amministrazione, utenti privati e mondo finanziario;
- ridurre i costi dell'attuale sistema dei pagamenti, grazie all'utilizzo di specifiche tecniche di interfacce standard, a vantaggio sia della pubblica amministrazione, sia dei privati.
- Garantire l'interazione fra i sistemi informativi delle pubbliche amministrazioni;
- Garantire l'integrazione dei metadati, delle informazioni e dei procedimenti amministrativi ai fini dell'erogazione di servizi finali integrati.
- operare sui flussi informativi senza interferire sui flussi finanziari né alterare le procedure di tesoreria ed i correlati rapporti con gli enti tesorieri;
- fornire uno strumento di riconciliazione automatica dei flussi degli incassi.

Effettuazione dei pagamenti con modalità informatiche

Sono state pubblicate le Linee guida per i pagamenti elettronici, ed una guida per l'adesione delle PA a PagoPA

La firma elettronica

La firma elettronica "debole" L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.

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. Il documento informatico sottoscritto con firma elettronica avanzata, formato nel rispetto delle regole tecniche, è riconosciuto valido fino a querela di falso.

L'art. 23-ter stabilisce che i documenti costituenti atti amministrativi, con rilevanza interna al procedimento amministrativo, sottoscritti con firma elettronica avanzata, fanno piena prova fino a querela di falso.

Va anche tenuto conto delle regole tecniche sulla firma elettronica avanzata, dettate agli artt. 55 e ss. del DPCM 22 febbraio 2013

La 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

La firma digitale Un particolare tipo di firma elettronica avanzata basata su Firma autenticata

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 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.

Firma autenticata 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

Il 1° luglio 2016 entrerà in vigore il Regolamento eIDAS – electronic IDentification Authentication and Signature – n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno. L'obiettivo dell'eIDAS è di agevolare la nascita in un quadro tecnico, economico e giuridico unico.

Nuove definizioni: identificazione elettronica, identificazione informatica, mezzi di identificazione elettronica, dati di identificazione personale, regime di identificazione elettronica, autenticazione, documento elettronico

Sono disciplinate solamente tre delle tipologie di firma elettronica individuate dal CAD (firma elettronica, avanzata e qualificata) insieme a tre sigilli elettronici (ripartiti allo stesso modo).

La firma elettronica rappresenta un insieme di dati che sono allegati o connessi, mediante una associazione logica, ad altri dati elettronici e sono utilizzati da una persona fisica per sottoscrivere elettronicamente un documento. Si evidenzia in questa nuova definizione soprattutto l'aspetto dichiarativo della firma piuttosto che l'elemento identificativo del sottoscrittore.

Allo stesso modo la firma elettronica avanzata viene connessa al firmatario e non più al documento.

Il valore giuridico (artt. 25-17):

1) La firma elettronica, ha gli effetti giuridici e il valore di prova riconosciuto dall'ordinamento nazionale alla firma autografa;

2) Le FEA emesse dagli Stati Membri possono essere utilizzate dai servizi on line del settore pubblico di un qualunque Stato Membro se sono conformi alle prescrizioni emanate dalla Commissione;

3) Se la FEQ è basata su un certificato qualificato rilasciato da uno Stato Membro è riconosciuta come FEQ in ogni Stato Membro

Viene introdotto per le imprese il sigillo elettronico (normale, avanzato e qualificato)

Il Regolamento prevede che per la firma elettronica qualificata sia verificato che il certificato qualificato debba essere "*valido al momento della firma*". Attualmente ciò non è garantito dalla normativa (tecnica) italiana che probabilmente dovrà essere aggiornata ed armonizzata

Dematerializzazione

Il termine "dematerializzazione" comporta quindi una riflessione generale sulle prassi amministrative che vada dalla gestione corrente delle attività alla conservazione permanente dei documenti.

La dematerializzazione riguarda: 1) i documenti nativi digitali; 2) le conversioni analogico/digitale; 3) riguarderà tutti i documenti, inclusi quelli contabili, di cui la legge impone la conservazione.

È di estrema importanza che tutte le fasi del processo di formazione del documento informatico e di firma dello stesso siano correttamente registrate e che i relativi log file siano conservati "a norma".

Il documento informatico è formato mediante una delle modalità previste espressamente dal DPCM 3 dicembre 2013

Il documento informatico assume la caratteristica di immodificabilità se formato in modo che forma e contenuto non siano alterabili durante le fasi di tenuta e accesso e ne sia garantita la staticità nella fase di conservazione.

L'art. 43 chiarisce che il documento informatico è valido e rilevante ad ogni effetto di legge SOLO se la riproduzione la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali.

Un idoneo sistema di conservazione deve essere in grado di garantire l'integrità dei dati oggetto di archiviazione e consentire l'esibizione e la valida produzione in giudizio a fini probatori dei documenti e delle relative informazioni a essi associate.

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. Ilocumento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, in modo da garantire 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.

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.

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 hanno piena efficacia se sottoscritti con firma digitale o altra firma elettronica qualificata.

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

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 tratte se la loro conformità all'originale non è espressamente disconosciuta.

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.

Le copie su supporto analogico di documenti informatici, anche sottoscritti con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta o se è attestata, in tutte le sue parti, da un pubblico ufficiale.

I duplicati informatici hanno il medesimo valore giuridico, ad ogni effetto di legge, del documento informatico da cui sono tratti.

Le copie e gli estratti informatici del documento informatico 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

Le modalità di associazione dei documenti ai rispettivi fascicoli, è una prerogativa di ogni singolo ente che a tal fine dovrà definire adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo.

La consultazione del fascicolo informatico deve garantire l'immodificabilità, il non ripudio, al leggibilità e l'integrità del documento informativo

L'intero sistema di conservazione digitale dei documenti informatici si fonda non solo sulle firme elettroniche, ma principalmente sulla marcatura temporale che garantisce quel fondamentale requisito di assicurare la validità giuridica nel tempo del documento. La marca temporale è da tenere ben distinta dalla firma digitale

Il Protocollo informatico

L'attività di protocollazione è quella fase del processo amministrativo che certifica provenienza e data di acquisizione del documento identificandolo in maniera univoca per mezzo dell'apposizione di informazioni numeriche e temporali.

L'art. 50 del DPR 445/2000 prevede che le pubbliche amministrazioni predispongono appositi progetti esecutivi per la sostituzione dei registri di protocollo cartacei con sistemi informatici conformi alle disposizioni del presente testo unico
A ciascuna AOO fa capo un unico protocollo informatico, attraverso il quale devono essere assicurati criteri uniformi di classificazione, di archiviazione e di comunicazione interna tra i differenti uffici della PA stessa, al fine di una gestione documentale coordinata.
Rilevante è la gestione del registro giornaliero di protocollo, che deve essere trasmesso, entro la giornata lavorativa successiva, al sistema di conservazione, al fine di garantirne l'immodificabilità del contenuto.
L'Agenzia per l'Italia digitale ha pubblicato le istruzioni relative alla produzione e alla conservazione del Registro giornaliero di protocollo.
Il sistema di protocollo informatico deve essere in grado di assicurare:
a) l'univoca identificazione ed autenticazione degli utenti;
b) la protezione delle informazioni relative a ciascun utente nei confronti degli altri;
c) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati;
d) la registrazione delle attività rilevanti ai fini della sicurezza svolte da ciascun utente, in modo tale da garantirne l'identificazione
La conservazione dei documenti rappresenta per le pubbliche amministrazioni una funzione di carattere istituzionale.
L'obbligo di conservazione dei documenti d'archivio è inteso a salvaguardare diritti soggettivi, interessi legittimi, il diritto d'accesso, la ricerca a fini storici, culturali e scientifici ed è finalizzato alla fruizione dei documenti per finalità amministrative e per interesse storico.
La conservazione: deve prevedere la cosiddetta conservazione dei bit (**Bit preservation**), cioè la capacità di accedere ai bit come erano stati originariamente registrati, anche in caso di degrado del supporto, di obsolescenza dell'hardware e/o disastri di sistema; deve essere garantita la conservazione logica (**Logical preservation**) intesa come la capacità di comprendere e utilizzare l'informazione in futuro, conservando il contenuto intellettuale anche in presenza di futuri cambiamenti tecnologici e di conoscenza.
I documenti che devono o comunque sono conservati 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
Il formato deve garantire immodificabilità e staticità del documento informatico.
Immodificabilità: caratteristiche che rende il contenuto non alterabile
Staticità: assenza di elementi dinamici (macroistruzioni, riferimenti) e assenza di strumenti di ausilio (annotazioni, revisioni, segnalibri)
La gestione del ciclo di vita di un documento informatico, deve essere efficiente e sicura.
Risulta decisivo avvalersi di un valido e completo **manuale di gestione documentale**, sottoposto a continuo aggiornamento, in ragione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e degli strumenti informatici utilizzati.
Le procedure e gli strumenti informatici devono essere in grado di governare ogni singolo accadimento che coinvolge la vita di un documento informatico
Il Responsabile della conservazione è la persona fisica inserita stabilmente nell'organico del soggetto produttore dei documenti, che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato.
Il Responsabile della conservazione, di concerto con il Responsabile della sicurezza, deve redigere il Piano della sicurezza del sistema di conservazione nell'ambito del Piano generale della sicurezza, nel rispetto delle misure previste dagli articoli da 31 a 36 del D.Lgs.n. 196/2003.
Il manuale della conservazione è il documento di riferimento in cui vengono descritte in modo dettagliato fasi di lavoro, strumenti e responsabilità che caratterizzano tutta l'attività di conservazione.

Lo scarto

L'operazione di distruzione dell'originale analogico sottoscritto (che comunque non può che intervenire solo dopo aver correttamente conservato la relativa copia informatica), deve essere valutata attentamente in ragione della possibilità o meno di vedersi contestata l'autenticità dell'originale ormai distrutto.

Il processo di distruzione del documento analogico coinvolge sia il Responsabile della conservazione che il Responsabile per il trattamento dei dati personali.
Il 14 dicembre 2016 la Direzione generale degli archivi ha diffuso le circolari 40 e 41 rispettivamente dirette agli Archivi di Stato e alle Soprintendenze archivistiche comunicando di fatto l'abrogazione della circolare 8 del 2004 che vietava la distruzione degli strumenti analogici I due provvedimenti prevedono che le strutture in questione approvino l'eliminazione del cartaceo solo dopo un'attenta verifica del rispetto delle procedure dettate dal CAD e dalle regole tecniche
Attualmente manca il coordinato ricorso a standard di sistemi di conservazione

Si pone una questione di effettiva costruzione qualitativa degli archivi e di interoperabilità tra i conservatori
Ai sensi dell'art. 44 bis CAD è possibile ottenere da AgID la qualifica di conservatori accreditati al fine di conseguire il riconoscimento del possesso dei requisiti del livello più elevato in termini di qualità e di sicurezza, chiedono l'accreditamento presso DigitPA.

Sicurezza

Solo 22 delle amministrazioni centrali analizzate e quasi nessuna delle Regioni, per non parlare dei Comuni, fa abbastanza per proteggersi. Ciò si deve in larga parte alla generalizzata ignoranza o sottostima da parte delle Amministrazioni del valore strategico ed economico delle informazioni da esse trattate.
Con le regole tecniche adottate DPCM del 1 aprile 2008 sono individuate le modalità che garantiscono l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture.
La casistica dei possibili eventi in grado di compromettere la funzionalità di un sistema informatico e l'integrità dei dati oltre ai possibili attacchi esterni al sistema, è varia:
- malfunzionamenti di sistemi, applicazioni e infrastrutture;
- eventi naturali di tipo accidentale, disastri:
- l'errore umano.

Con l'espressione "**continuità operativ**a" viene indicata la capacità dell'organizzazione di proseguire l'esercizio delle proprie attività istituzionali anche di fronte ad eventi disastrosi che possono colpirla.
Con l'espressione "**disaster recovery**" viene indicato il piano finalizzato ad assicurare il funzionamento dei processi ICT con mezzi alternativi a quelli impiegati in condizioni normali.
La CO ed il DR travalicano l'ambito informatico e vanno ad interessare l'intera funzionalità dell'organizzazione amministrativa.
Agid ha messo a disposizione delle PPAA uno Strumento di Autovalutazione
Nelle Linee guida viene sempre richiamato il rispetto degli artt. 31 e 34 del d.lgs. 196/2003, il quale più volte è intervenuto come per quanto riguarda i back up e «periodo di ritenzione»

Il 20 gennaio 2016 è stato approvato dal Consiglio dei Ministri lo schema di decreto per la Riforma del CAD
Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico.
Soltanto la motivata impossibilità tecnico-economica a reperire software liberi o a codici sorgente aperto, consente l'acquisizione di software proprietario.

Il riuso

Per riuso si intende il grado con cui un modulo o un'altra componente software può essere riusato in uno o più di un programma software.

Il riuso del software è un concetto applicabile all'insieme delle componenti del prodotto software, definito come "*l'insieme di programmi, procedure, regole, documenti, pertinenti all'utilizzo di un sistema informatico*"

Sitografia:

- http://www.qualitapa.gov.it/
- http://www.formez.it/
- http://www.rispondipa.it/
- http://www.magellanopa.it/
- http://www.forumpa.it/
- http://www.agid.gov.it/
- http://www.spid.gov.it/
- http://www.anticorruzione.it/portal/public/classic/

Documentazione

- Contenuti minimi web
- Linee Guida siti Web 2011
- Modello di dichiarazione di accessibilità
- Manuale applicativo strategie di acquisizione delle forniture ict
- La trasparenza sui siti web della PA - Linee guida del Garante
- Linee Guida Mettiamoci la Faccia
- Rapporto Monitor 2014
- Nuovi requisiti legge Stanca
- Piano di comunicazione PA
- Privacy e lavoro vademecum 2015 Garante
- Linee guida Disaster Recovery
- Raccomandazioni DigitPA sul cloud
- Agid – Caratteristiche dei sistemi cloud per le PA
- Manuale di gestione documentale