DigitPA

Elementi generali del nuovo Codice dell'Amministrazione Digitale

Ing. Elena Tabet
DigitPA

Perugia, 11 aprile 2011

Riforma del CAD - Impostazione

- Rinnovamento del quadro normativo del D.lgs 82/2005
- Adeguamento dello scenario tecnologico
- Coerenza rispetto alla riforma 150/2009
- Nuovi diritti per cittadini ed imprese
- Orizzonte temporale: 2012

Principi ispiratori 1/2

- Modifica, integrazione e precisazione del quadro normativo per realizzare il pieno valore giuridico delle transazioni digitali (per esempio il valore della stampa su carta di un documento originato in forma digitale e la semplificazione dei meccanismi di riconoscimento in linea del soggetto che attiva una transazione digitale)

- Ampliamento della platea dei destinatari

- Standard e regole tecniche per assicurare l'interoperabilità delle transazioni e la piena operatività della riforma (i vari strumenti diventano un sistema integrato che consente varietà dei punti di accesso, molteplicità di dispositivi e risposte coordinate)

- Effettività della riforma: misure premiali, quantificazione dei risparmi dovuti all'introduzione dell'innovazione, sanzioni (art. 12)

Principi ispiratori 2/2

- Incentivazione dell'innovazione: possibilità di riutilizzare i risparmi per finanziare nuovi progetti di innovazione e per premiare il personale (art. 15) – dividendo di efficienza legato all'innovazione

- Scadenze cogenti per la messa a disposizione dei servizi con meccanismi di incentivi e disincentivi per i responsabili dell'eventuale mancato rispetto delle scadenze

- Strumenti di accompagnamento messi a disposizione dalle strutture MIPAI:
  - Informazione agli utenti sui servizi disponibili (quale amministrazione presta quali servizi in linea e attraverso quali canali è contattabile, ma anche come l'utente può esprimere il proprio grado di soddisfazione per i servizi erogati)

  - Miglioramento dell'assistenza alle PA e ai cittadini (a partire dai call center per avere notizie e risolvere questioni specifiche)

Destinatari

Ora:

- Pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165
- nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione
- Società, interamente partecipate da enti pubblici o con prevalente capitale pubblico

Prima:

- *Pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, salvo che sia diversamente stabilito, nel rispetto della loro autonomia organizzativa e comunque nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione*

Elementi chiave nei rapporti fra privati

- Il Codice stabilisce dei criteri regolatori di carattere generale validi nei rapporti fra privati, con il mondo delle imprese, dei professionisti, delle banche, delle assicurazioni…
- Alcune innovazioni hanno un raggio di azione che si estende oltre la pubblica amministrazione:
    - Validità dei documenti informatici artt. 20-23
        - Duplicati e copie informatiche di documenti informatici
        - Copie informatiche di documenti analogici
        - Copie analogiche di documenti informatici
        - Regole tecniche entro 12 mesi
    - Conservazione artt. 43-44
        - Responsabile della conservazione
        - Soggetti pubblici o privati
        - Conservatori accreditati
        - Regole tecniche entro 12 mesi
    - Posta elettronica certificata artt. 6, 40 bis, 48 e 65

Elementi chiave nei rapporti con la PA 1/3

- I cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le pubbliche amministrazioni, con i soggetti destinatari, e con i gestori di pubblici servizi (con le pubbliche amministrazioni e con i gestori di pubblici servizi statali) (art. 3)

- 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

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

Elementi chiave nei rapporti con la PA 2/3

- Si allargano e si rafforzano gli ambiti in cui gli scambi fra amministrazione e cittadini sono basati esclusivamente sulle tecnologie dell'informazione e della comunicazione:
  - Pagamenti verso le PA (centrali e locali) art. 5
    - Deve essere consentito il pagamento per via telematica, anche attraverso intermediari privati di servizi
    - Possibili strumenti di pagamento: carte di debito/credito, prepagate, altri strumenti elettronici di pagamento
  - Comunicazioni fra imprese e PA art. 5 bis
    - Avvengono solo per via telematica
    - Lo sportello unico delle attività produttive eroga servizi solo in via telematica
  - Pubblicità legale art. 54 4-bis, conferma quando previsto dall' art. 32 L. 69/2009

Elementi chiave nei rapporti con la PA 3/3

- Costante verifica del percorso di riforma
- I cittadini possono valutare l'operato dell'amministrazione, la qualità e l'efficacia dei servizi erogati in rete:
  - migliore soddisfazione delle esigenze degli utenti
  - completezza del procedimento
  - certificazione dell'esito
  - accertamento del grado di soddisfazione dell'utente
- Le amministrazioni devono rendere disponibili strumenti per la valutazione dei dirigenti e delle organizzazioni, consentendo di fatto al cittadino di essere concretamente partecipe al miglioramento della qualità dei servizi
- Strumenti idonei alla rilevazione immediata, continua e sicura del giudizio degli utenti quando usufruiscono di un servizio online.

Identificazione informatica 1/2

- Per dispiegare servizi in rete con assoluta sicurezza ed affidabilità, è necessario avere la certezza che ad un utenza digitale (cioè, ad esempio, ad un *nomeutente* e ad una *password*) sia associato univocamente un soggetto fisico o giuridico, sia esso cittadino o azienda.
- Identificazione informatica: identificazione univoca di un soggetto per via telematica che consiste nella validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad esso, consentendone l'individuazione nei sistemi informativi
- Prerequisito decisivo per dispiegare efficacemente il processo di erogazione online di molti servizi pubblici
- Necessaria a consentire una piena comunicazione in via telematica fra cittadino e amministrazioni

Identificazione informatica 2/2

- Secondo l'articolo 64 le amministrazioni possono consentire l'accesso ai servizi online, che richiedono identificazione informatica, da parte di cittadini e imprese oltre che mediante la carta di identità elettronica (CIE) e la carta nazionale dei servizi (CNS), anche **utilizzando strumenti diversi per individuare il soggetto richiedente**
- Art 65 (*Istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica)* c e c-bis:
  - Sottoscritte con firma digitale il cui certificato è rilasciato da un certificatore accreditato;
  - CIE o CNS;
  - autore identificato informaticamente
  - articolo 38, comma 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (invio dell'istanza con copia fotostatica del documento di identità);
  - Invio tramite casella di posta elettronica certificata purché le credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica

Firme elettroniche

CQ: Certificato Qualificato

- Documento informatico che lega i dati personali del titolare alla chiave pubblica utilizzata nella verifica della firma.
- Oggetto di norme comunitarie e nazionali
- Può contenere titoli o ruoli ricoperti in una organizzazione
- Può contenere limiti d'uso o di valore
- Rilasciato da un soggetto sottoposto a vigilanza ex art. 31 del CAD

SSCD: Secure Signature Creation Device

- Dispositivo sicuro per la generazione della firma
- Smartcard – token usb – HSM
- valutato e certificato sulla base di una valutazione conforme alla Direttiva 1999/93/EC e approvata da organismi europeo accreditati

Firme elettroniche

Liberamente valutabile

FIRMA ELETTRONICA

Insieme di dati usati per l'identificazione

Inversione dell'onere della prova – valida fino a querela di falso

FIRMA ELETTRONICA AVANZATA ([1])

FE + connessione univoca con il soggetto, mezzo a controllo esclusivo

([1]) Vi troveranno collocazione , con appositi DPCM, sistemi alternativi alla firma elettronica qualificata e digitale che, per il contesto di utilizzo, necessitano di un diverso valore probatorio.

Soddisfa il requisito della forma scritta ex art. 1350 p.ti 1-12.

FIRMA ELETTRONICA QUALIFICATA

FEA + SSCD + certificato qualificato

FIRMA DIGITALE ([2])

FEA + certificato qualificato + crittografia asimmetrica

([2]) E utile per il sistema di firma remota di interesse per il mondo bancario, assicurativo e sanitario

Tipologie di firme

SARANNO EMANATE NUOVE REGOLE TECNICHE

Documento informatico

documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (contrapposto al documento analogico)

20 – Documento informatico

3. Le regole tecniche per la formazione, per la trasmissione, la conservazione, la copia, la duplicazione, la riproduzione e la validazione temporale dei documenti informatici, nonché quelle in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica avanzata, sono stabilite ai sensi dell'articolo 71. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle regole tecniche sulla validazione temporale.

5-bis. Gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti a tutti gli effetti di legge a mezzo di documenti informatici, se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'articolo 71.

VALIDITA'

- **Liberamente valutabile in giudizio se sprovvisto di firma o con firma elettronica**
- **Piena prova fino a querela di falso se sottoscritto con firma elettronica avanzata, qualificata o digitale**
- **Se contenente le scritture private di cui all'art. 1350 c.c. è richiesta la firma elettronica qualificata o digitale a pena di nullità**

Documento informatico

copia informatica di documento analogico: il documento informatico avente contenuto identico a quello del documento analogico da cui è tratto

22 – Copie informatiche di documento analogico

1. I documenti informatici contenenti copia di atti pubblici, scritture private e documenti in genere, compresi gli atti e documenti amministrativi di ogni tipo formati in origine su supporto analogico, spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia, ai sensi degli articoli 2714 e 2715 del codice civile, se ad essi è apposta o associata, da parte di colui che li spedisce o rilascia, una firma digitale o altra firma elettronica qualificata. La loro esibizione e produzione sostituisce quella dell'originale.

23-ter Documenti amministrativi informatici

3. Le copie su supporto informatico di documenti formati dalla pubblica amministrazione in origine su supporto analogico ovvero da essa detenuti, hanno il medesimo valore giuridico, ad ogni effetto di legge, degli originali da cui sono tratte, se la loro conformità all'originale è assicurata dal funzionario a ciò delegato nell'ambito dell'ordinamento proprio dell'amministrazione di appartenenza, mediante l'utilizzo della firma digitale o di altra firma elettronica qualificata e nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 …

È un documento informatico formato dal testo di un documento su carta (OCR di una scansione)

VALIDITA'

- **Con attestazione di conformità da parte di notaio o altro pubblico ufficiale, stessa efficacia probatoria degli originali**
- **Senza attestazione di conformità, stessa efficacia probatoria degli originali se non espressamente disconosciuta**
- **Nel caso di documenti della PA è sempre richiesta l'attestazione di conformità da parte del pubblico ufficiale**

Documento informatico

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

22 – Copie informatiche di documento analogico

2. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, con dichiarazione allegata al documento informatico e asseverata secondo le regole tecniche stabilite ai sensi dell'articolo 71..

3. Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta.

È un documento informatico formato dalla immagine di un documento su carta (scansione)

VALIDITA'

- **Con attestazione di conformità da parte di notaio o altro pubblico ufficiale, stessa efficacia probatoria degli originali**
- **Senza attestazione di conformità, stessa efficacia probatoria degli originali se non espressamente disconosciuta**

Documento informatico

La copia informatica di documento analogico e la copia per immagine su supporto informatico di documento analogico sono idonee ad assolvere gli obblighi di conservazione

22 – Copie informatiche di documento analogico

5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

6. Fino alla data di emanazione del decreto di cui al comma 5 per tutti i documenti analogici originali unici permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.

- **Con DPCM saranno individuate le tipologie di documenti originali "unici" che devono essere conservate in originale cartaceo**
- **Fintantoché non viene emanato il suddetto DPCM è necessario conservare l'originale cartaceo o la copia con l'attestazione di conformità da parte di notaio o altro pubblico ufficiale**

Documento informatico

copia analogica di documento informatico: il documento su carta avente contenuto identico a quello del documento informatico da cui è tratto

23 – Copie analogiche di documenti informatici

1. Le copie su supporto analogico di documento informatico, anche sottoscritto con firma elettronica avanzata, qualificata o digitale, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale in tutte le sue componenti è attestata da un pubblico ufficiale a ciò autorizzato.

2. Le copie e gli estratti su supporto analogico del documento informatico, conformi alle vigenti regole tecniche, hanno la stessa efficacia probatoria dell'originale se la loro conformità non è espressamente disconosciuta. Resta fermo, ove previsto l'obbligo di conservazione dell'originale informatico.

23-ter Documenti amministrativi informatici

5. Al fine di assicurare la provenienza e la conformità all'originale, sulle copie analogiche di documenti informatici, è apposto a stampa, sulla base dei criteri definiti con linee guida emanate da DigitPA, un contrassegno generato elettronicamente, formato nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 e tale da consentire la verifica automatica della conformità del documento analogico a quello informatico.

È la stampa di un documento informatico

VALIDITA'

- **Con attestazione di conformità da parte di notaio o altro pubblico ufficiale, stessa efficacia probatoria degli originali**
- **Senza attestazione di conformità, stessa efficacia probatoria degli originali se non espressamente disconosciuta**
- **La stampa di documenti della PA deve contenere un contrassegno che garantisce la conformità all'originale**

Posta elettronica certificata 1/5

- Evidente il rilievo che il Codice dà alla posta elettronica certificata
- 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
- Principale mezzo di comunicazione per il cittadino nella presentazione di istanze verso le pubbliche amministrazioni
- Lo strumento che le pubbliche amministrazioni sono tenute ad utilizzare quando a fare richiesta in tale senso è il cittadino stesso
- Strumento fondamentale per le comunicazioni effettuate da e verso le pubbliche amministrazioni da parte delle imprese

Posta elettronica certificata 2/5

- La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata, equivale, salvo che la legge non disponga diversamente (nei casi consentiti dalla legge) alla notificazione per mezzo della posta

- Le comunicazioni di documenti tra le pubbliche amministrazioni avvengono (di norma) mediante l'utilizzo della posta elettronica e sono valide ai fini del procedimento amministrativo una volta che ne sia verificata la provenienza
  - Segnatura di protocollo
  - Firma digitale o firma elettronica qualificata
  - PEC

Posta elettronica certificata 3/5

- Le comunicazioni inviate via PEC devono essere protocollate (art. 40 bis)
- Obbligo per le amministrazioni a pubblicare nell'Indice delle Pubbliche amministrazioni –IPA –almeno una PEC per ogni registro di protocollo
- Vengono limitati i casi in cui è richiesta la sottoscrizione con firma digitale, casi da individuare con Decreto MIPAI e Semplificazione
- Le istanze possono essere inviate da tutte le caselle di posta elettronica certificata rilasciate previa identificazione del titolare
- Le amministrazioni possono accedere agli elenchi di titolari di casella di posta elettronica certificata (regole tecniche con Garante)

Posta elettronica certificata 4/5

- Le amministrazioni:
  - devono utilizzare la posta certificata per tutte le comunicazioni che necessitano di una ricevuta di invio e di una di consegna – ciò che finora veniva fatto con la raccomandata A/R – verso cittadini, professionisti, imprese che hanno preventivamente comunicato il proprio di indirizzo di PEC;
  - devono pubblicare i propri indirizzi di posta elettronica certificata nell'Indice delle Pubbliche amministrazioni, che costituisce la rubrica degli indirizzi delle amministrazioni, accessibile e consultabile da tutti all'indirizzo www.indicepa.gov.it;

- I cittadini:
  - accettano automaticamente l'invio di atti e provvedimenti che li riguardano da parte delle pubbliche amministrazioni una volta dichiarato il proprio indirizzo PEC
  - possono trovare gli indirizzi di PEC dei diversi enti all'indirizzo: www.indicepa.gov.it.

Posta elettronica certificata 5/5

- Le modifiche normative sono state accompagnate da azioni volte alla diffusione della PEC fra i cittadini e fra i professionisti

- PEC Avvocati
- PEC per gli iscritti agli Ordini professionali

- Ad aprile 2010 è stata avviata l'iniziativa CEC-PAC Postacertificat@: PEC gratuita ai cittadini per le comunicazioni con le PA iscritte all'indice IPA

- In fase di realizzazione: PEC per i dipendenti pubblici per tutte le comunicazioni con gli Enti di riferimento (PAC,INPS, INPDAP…)

- In fase di realizzazione: PEC per le comunicazioni MIUR-supplenti

Siti web pubblici

- Si rafforza il percorso avviato con la Direttiva MIPAI 8/2009 e le Linee guida per i siti web della PA
- Siti pubblici e trasparenza (art. 54)
  - Il contenuto obbligatorio dei siti viene arricchito – pubblicazione integrale di tutti i concorsi
- Pubblicazione di moduli/formulari art. 57

  "Le pubbliche amministrazioni non possono richiedere l'uso di moduli e formulari che non siano stati pubblicati; in caso di omessa pubblicazione, i relativi procedimenti possono essere avviati anche in assenza dei suddetti moduli o formulari"
  - la mancata pubblicazione è rilevante ai fini della misurazione e della valutazione delle performance

Siti web delle amministrazioni

- Sportello telematico per cittadini, imprese e professionisti
- Comunicazione istituzionale e comunicazione di servizio
- Luogo in cui la PA pubblica gli strumenti (PEC, modulistica, servizi) a disposizione dei cittadini per l'interazione basata su tecnologie ICT
- Necessità di razionalizzare e rendere coerenti i siti delle amministrazioni e di garantire un'interfaccia omogenea
- Principale interfaccia di accesso, da parte dei cittadini, ai datti delle amministrazioni

I dati delle amministrazioni 1/2

- L'informazione pubblica - insieme delle informazioni e dei dati raccolti, prodotti e gestiti dalla pubblica amministrazione nell'esercizio delle proprie attività istituzionali - rappresenta una risorsa che deve essere disponibile sia a tutte le amministrazioni sia ai cittadini.

- Scambio di dati fra amministrazioni art. 58
  - Le amministrazioni non possono richiedere informazioni di cui già dispongono: si spostano i dati e non le persone
  - Le amministrazioni titolari di dati predispongono apposite convenzioni aperte per assicurare l'accessibilità dei dati
  - I dati sono disponibili gratuitamente, eventuali elaborazioni dei dati possono essere remunerate

I dati delle amministrazioni 2/2

- Dati aperti e formati aperti (artt. 52 e 68)
- Le amministrazioni devono divulgare e valorizzare i dati pubblici, secondo i principi dell'open government e degli open data
- Tutte le attività dei governi e delle amministrazioni dello stato devono essere aperte e disponibili per favorire azioni efficaci e garantire un controllo pubblico sull' operato
- Dati aperti: liberamente accessibili senza restrizioni di copyright, brevetti o altre forme di controllo che ne limitino la riproduzione
- Formato aperto: definito da specifiche pubbliche non proprietarie, liberamente accessibili, senza restrizioni legali per l'utilizzo.

Il Sistema pubblico di connettività

- SPC: insieme di infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione (art. 73)
- Rete federata, policentrica, non gerarchica della pubblica amministrazione
- Garantisce:
  - interazione della pubblica amministrazione centrale e locale con tutti gli altri soggetti connessi a Internet
  - servizi di connettività condivisi dalle pubbliche amministrazioni interconnesse
  - interoperabilità tra tutte le reti delle pubbliche amministrazioni esistenti
- Partecipano ad SPC tutte le amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165
- Possono partecipare ad SPC anche soggetti privati gestori di servizi pubblici o chi persegue finalità di pubblico interesse

Sicurezza e continuità del servizio

- La diffusione delle tecnologie informatiche nelle PA e la tenuta di archivi informatizzati rende necessario:
  - Individuare procedure per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture
  - Garantire la continuità del servizio anche quando erogato mediante tecnologie ICT (art. 50 bis)
  - Individuare le procedure da mettere in atto in situazioni di emergenza, che devono riguardare le risorse umane, le risorse strumentali, le strutture e le infrastrutture

Definizione di continuità operativa e di disaster recovery

Dalle "Linee guida per la continuità operativa della Pubblica Amministrazione" (Quaderno n. 28 DigitPA):

- *Continuità operativa: insieme di attività volte a minimizzare gli effetti distruttivi di un evento che ha colpito una organizzazione o parte di essa con l'obiettivo di garantire la continuità delle attività in generale. Include il Disaster Recovery.*

- *Disaster Recovery: insieme di attività volte a ripristinare lo stato del sistema informatico o parte di esso, compresi gli aspetti fisici e organizzativi e le persone necessarie per il suo funzionamento, con l'obiettivo di riportarlo alle condizioni antecedenti a un evento disastroso.*

La continuità operativa

- La continuità operativa si propone di trattare in modo unitario qualunque problema di discontinuità del servizio che assuma rilevanza per durata e dannosità
- Alcune soluzioni di continuità operativa permettono di affrontare anche problemi di natura ordinaria (fermi contenuti o programmati)
- Nel settore pubblico:
  - La pubblica amministrazione è tenuta ad assicurare la continuità dei propri servizi per garantire il corretto svolgimento della vita nel Paese (si ricorda l'art. 97 della Costituzione ed il principio di buon andamento dell'amministrazione, da rispettare anche se si utilizzano tecnologie ICT)

Norme in materia di continuità operativa

- Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196)

- Decreto legislativo 30 dicembre 2010, n. 235 (Gazz. Uff. 10 gennaio 2011, n. 6):

  Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.

Gli obblighi per i dati personali (Decreto legislativo 30 giugno 2003, n. 196)

- Articolo 31

  - I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Gli obblighi per i dati personali (Decreto legislativo 30 giugno 2003, n. 196)

- **Art. 34 - Trattamenti con strumenti elettronici**

- 1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato [B], le seguenti misure minime:
- a. autenticazione informatica;
- b. adozione di procedure di gestione delle credenziali di autenticazione;
- c. utilizzazione di un sistema di autorizzazione; d. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e. protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- g. tenuta di un aggiornato documento programmatico sulla sicurezza;
- h. adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

CAD

- Il Dlgs introduce nel CAD l'articolo 50-bis (Continuità operativa):
- 1.In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.
- 2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.
- 3. A tali fini, le pubbliche amministrazioni definiscono :
  a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;
  b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.
- 4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.".

Cosa si intende per “disastro”

- **Disastro** Una calamità improvvisa e non pianificata che causa gravi danni o perdite.

Gli eventi critici che possono produrre un disastro

- Eventi calamitosi
- Problemi nella catena di approvvigionamento
- Fermi nella alimentazione elettrica degli edifici
- Guasti nella rete
- Incendi
- Inagibilità dei locali per qualunque causa
- Fermi informatici: guasti critici dei server, malfunzionamenti nei sistemi di autenticazione e accesso, attacchi informatici, ecc.
- …
- Combinazioni di eventi singoli

Come affrontare un situazione di disastro

- E’ necessario predisporre un insieme di procedure e di dati raccolti in un “Piano di continuità operativa”
- La componente informatica costituisce uno degli elementi di questo piano ed è precisata in un “Piano di disaster recovery”

Il Piano di continuità operativa (PCO)

Ogni piano deve definire:

1. Scopo e campo di applicazione, dove si identificano gli elementi fisici (quali le sedi, le aree all'interno delle sedi, il data center, ecc.) e funzionali (le attività di business o i servizi) dell'organizzazione coperti dal piano
2. Obiettivi di continuità degli elementi coperti dal piano
3. Ruoli e responsabilità nella gestione dell'emergenza, con particolare evidenza dei ruoli decisionali di vertice dell'organizzazione;
4. Criteri di attivazione delle procedure di emergenza (le condizioni che determinano la dichiarazione di disastro)
5. Procedure di attuazione in risposta alla condizione di di emergenza (la reperibilità del personale chiave, le modalità di comunicazione ai dipendenti, le modalità di comunicazione agli esterni interessati – nel caso di PA: cittadini, imprese, altre PA-, il piano di disaster recovery);
6. Flusso di informazioni e processi di documentazione
7. Modalità di verifica e di aggiornamento del Piano

“Buone regole”

La continuità operativa rappresenta la garanzia di funzionalità di un’organizzazione e questo è tanto più evidente per una pubblica amministrazione.

Il porre attenzione a come affrontare una situazione di emergenza, organizzandosi per rispondere in modo ordinato e proceduralizzato all’emergenza è un’attività che non implica sempre e comunque costi aggiuntivi, ma certamente esige attenzione e valutazione adeguati. Spesso, infatti, “buone regole” possono già costituire un primo passo significativo per l’innalzamento del proprio livello di continuità.

Riferendosi agli aspetti ICT, talvolta anche rivedere alcune procedure che si considerano routinarie e scontate può portare a un aumento della continuità: un esempio classico sono le attività e l’organizzazione dei salvataggi dei dati, il backup.

“Buone regole”: il backup dei dati

Quali contenuti e, soprattutto, quali modalità dovrebbe avere/verificare una reale politica di backup? Di seguito una sintesi:

1. Tempistica

La tempistica è la periodicità con cui vanno eseguiti i salvataggi dei dati.

2. Periodo di ritenzione

I salvataggi devono avere un periodo di ritenzione (anche illimitato) passato il quale vengono eliminati.

Il periodo di ritenzione consente il recupero periodico degli spazi o dei supporti usati per il salvataggio dei dati.

3. Responsabilità

Và identificato la funzione o la divisione responsabile per l’esecuzione delle procedure relative alla politica di backup.

4. Verifica salvataggi

Periodicamente la politica deve prevedere di effettuare un ripristino dei dati salvati per verificare la bontà dei backup effettuati.

5. Lista dei dati Salvati

Devono essere elencati tutti i dati oggetto del salvataggio a cui la politica fa riferimento.

6. Archiviazioni

La politica può prevedere che periodicamente tutti o parte dei dati salvati siano oggetto di archiviazione su dispositivi che ne preservano l’integrità per lunghi periodi (tipicamente anni).

7. Ripristino (Restore)

La politica deve contenere l’insieme delle procedure da eseguire in caso di ripristino dei dati, in termini di modalità, sequenza e controllo dei dati ripristinati

8. Ubicazione

In caso di uso di supporti removibili di salvataggio, la politica deve prevedere il tipo di conservazione e l’ubicazione dei supporti (armadi ignifughi, caveau ecc…).

I tempi della riforma 1/3

- Entro 3 mesi

  Le amministrazioni utilizzano la PEC per le comunicazioni che richiedono una ricevuta di consegna

- Entro 4 mesi

  Le amministrazioni individuano un unico ufficio responsabile dell'attività ICT

- Entro 6 mesi

  - Le PA centrali pubblicano sui propri siti istituzionali i bandi di concorso
  - Le amministrazioni consentono ovunque i pagamenti ad esse spettanti per via telematica
  - Le amministrazioni e le imprese comunicano tra loro esclusivamente per via telematica

I tempi della riforma 2/3

- Entro 12 mesi
  - Sono emanate le regole tecniche per dare piena validità alle copie cartacee e, soprattutto, a quelle digitali dei documenti informatici, dando così piena effettività al processo di dematerializzazione dei documenti della PA
  - Sono emanate le regole tecniche per la conservazione sostitutiva dei documenti in forma digitale dando il via agli archivi informatizzati
  - Le pubbliche amministrazioni non possono richiedere l'uso di moduli e formulari che non siano stati pubblicati sui propri siti istituzionali
  - Il cittadino fornisce una sola volta i propri dati alla pubblica amministrazione. Sarà onere delle amministrazioni (in possesso dei dati) assicurare, tramite convenzioni, l'accessibilità delle informazioni alle altre amministrazioni richiedenti

I tempi della riforma 3/3

- Entro 12 mesi
  - Definite le basi di dati di interesse nazionale
  - Emanate tutte le regole tecniche previste dal CAD
  - Le regole del nuovo CAD si applicheranno, mediante un apposito DPCM, anche alla Presidenza del Consiglio dei Ministri e all'Amministrazione finanziaria

- Entro 15 mesi
  Le PA predispongono appositi piani di emergenza idonei ad assicurare, in caso di eventi disastrosi, la continuità delle operazioni indispensabili a fornire i servizi e il ritorno alla normale operatività

La redazione delle regole tecniche

Per ciascun ambito del Codice si stanno avviando dei gruppi di lavoro sia per la redazione delle regole tecniche sia per il monitoraggio dello stato di avanzamento dell'attuazione nelle amministrazioni

Le attività dei Gruppi di Lavoro sono essenziali alla costruzione e alla manutenzione di regole e guide operative che non solo siano condivise ma soprattutto che siano la base di una comune cultura di informatizzazione dei servizi di interesse collettivo

Il percorso delle regole tecniche

Il percorso di emanazione delle regole tecniche è il seguente:

1. Costituzione dei Gruppi di Lavoro
   - coordinamento DigitPA
   - rappresentanti delle Amministrazioni competenti in materia come previste dal CAD
   - rappresentanti di PAC, Regioni, EE.LL.
   - rappresentanti del mondo scientifico e del mercato
2. Redazione del documento preliminare
3. Condivisione:
   - Consultazione pubblica mediante forum
   - Recepimento di osservazioni di stakeholders selezionati
4. Emanazione documento definitivo
5. Avvio del monitoraggio del processo di emanazione delle regole tecniche
6. Rapporto trimestrale di monitoraggio del processo di emanazione delle regole tecniche

Stato di attuazione

1. Identificazione degli ambiti CAD prioritari **FATTO**
2. Costituzione dei Gruppi di Lavoro **FATTO**
3. Identificazione dei prodotti
   (Regole tecniche/linee guida) **FATTO**
4. Impostazione degli indici dei documenti **FATTO**
5. Redazione testo iniziale
6. Validazione del testo con i soggetti pubblici coinvolti
7. Invio ai soggetti privati (stakeholders) e loro commenti
8. Consultazione pubblica (web)
9. Raccolta pareri dovuti (Consiglio di Stato,
   Corte dei Conti, Garante, etc.)
10. Notifica alla Comunità Europea
11. Redazione testo finale emanazione

I gruppi di lavoro avviati

- Regole tecniche su formazione, tenuta e conservazione del documento informatico
- Regole tecniche identità digitali
- Regole tecniche banche dati
- Linee Guida per la continuità operativa e infrastrutture critiche nella P.A.
- Regole tecniche gestione documento informatico e gestione flussi documentali
- Regole tecniche firma digitale

Chi partecipa ai gruppi di lavoro

- Garante per la protezione dei dati personali
- Amministrazioni centrali (MEF, MIBAC, Giustizia…)
- Agenzie ed Istituti
- ISTAT
- Rappresentati di Regioni ed Enti locali
- Organismi di standardizzazione
- Associazioni di categoria (ABI, Assintel, Assinform…)
- Consiglio Nazionale del Notariato
- Ordini professionali
- Università

Per maggiori informazioni

- **www.digitpa.gov.it**
- **tabet@digitpa.gov.it**
- **continuita_operativa@digitpa.gov.it**